

IBM OpenPages with Watson
Version 8.2.0

Administrator's Guide



Note

Before using this information and the product it supports, read the information in [“Notices” on page 1125](#).

Product Information

This document applies to IBM OpenPages with Watson 8.2.0 and may also apply to subsequent releases.

Licensed Materials - Property of IBM Corporation.

© Copyright IBM Corporation, 2003, 2023.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Note.....	iii
Introduction.....	xxxi
IBM OpenPages with Watson	xxxii
How IBM OpenPages with Watson can help.....	xxxii
Shared content management and common repository.....	xxxiii
Dynamic decision support with Cognos.....	xxxiii
Simple configuration and localization.....	xxxiii
Flexible automation.....	xxxiii
Web services-based integration.....	xxxiii
Installation locations for IBM OpenPages with Watson.....	xxxiii
Special characters in passwords.....	xxxvi
Variables and placeholders.....	xxxvii
Chapter 1. What's new?.....	1
New and changed features in version 8.2.0.4.....	1
New and changed features in version 8.2.0.3.....	2
New and changed features in version 8.2.0.2.....	4
New and changed features in version 8.2.0.1.....	6
New and changed features in version 8.2.....	9
New and changed features in version 8.1.0.1	14
New and changed features in version 8.1.0.....	16
New and changed features in version 8.0.0.3.....	20
New and changed features in version 8.0.0.2.....	21
New and changed features in version 8.0.0.1.....	23
New and changed features in version 7.4.0.....	24
Platform enhancements.....	24
Administration and serviceability enhancements.....	25
New features in version 7.3.0.3.....	27
New features in version 7.3.0.2.....	27
New features in version 7.3.0.1.....	28
New features in version 7.3.0.....	29
Chapter 2. OpenPages for IBM Cloud Pak for Data.....	33
Documentation for IBM OpenPages for IBM Cloud Pak for Data administrators.....	33
Managing users and groups within IBM Cloud Pak for Data.....	35
Adding users	35
Managing access to OpenPages instances	36
How users and groups are synchronized from Cloud Pak for Data to OpenPages.....	36
Configuring the user and group synchronization job.....	39
Checking running synchronization jobs.....	40
Files and directories in IBM OpenPages for IBM Cloud Pak for Data.....	40
Starting and stopping application servers in IBM OpenPages for IBM Cloud Pak for Data.....	41
Cognos Analytics and OpenPages for Cloud Pak for Data.....	42
Adding Cognos to OpenPages.....	43
Installing tools and utilities in Cloud Pak for Data.....	44
Configuring IBM OpenPages for IBM Cloud Pak for Data.....	45
Preparing the instance.....	46
Backing up changes and implementing them across replicas.....	46
Backing up IBM OpenPages for IBM Cloud Pak for Data.....	47

Performing an online backup.....	47
Performing an offline backup.....	49
Backing up custom files in IBM OpenPages for IBM Cloud Pak for Data.....	50
Restoring IBM OpenPages for IBM Cloud Pak for Data.....	52
Migrating IBM OpenPages for IBM Cloud Pak for Data to another instance.....	54
Changing the password of the OPSys user in IBM OpenPages for IBM Cloud Pak for Data.....	57
Changing the password of the Liberty keystore in IBM OpenPages for IBM Cloud Pak for Data.....	58
Configuring server certificates in IBM OpenPages for IBM Cloud Pak for Data.....	59
Replacing the self-signed certificate for the cluster.....	59
Setting up a CA certificate for OpenPages.....	60
Importing a certificate into the local trust store on IBM OpenPages for IBM Cloud Pak for Data.....	61
Changing the data encryption key for IBM OpenPages for IBM Cloud Pak for Data.....	62
Backing up the current encryption key.....	62
Backing up OpenPages.....	63
Decrypting data with the current encryption key.....	63
Generating a new secret key.....	64
Updating OpenShift with the new key.....	64
Restarting the application servers.....	65
Encrypting data with the new key.....	65
Restarting the application servers.....	66
Logging in to the database in IBM OpenPages for IBM Cloud Pak for Data.....	67
Updating IBM OpenPages Model Risk Governance for integration with OpenScale.....	67
Updating IBM OpenPages Financial Controls Management.....	69

Chapter 3. System Admin Mode (SAM).....71

Enabling and disabling System Admin Mode.....	71

Chapter 4. Users, groups, and domains.....73

Planning user administration.....	73
The Super Administrator.....	75
Creating a Super Administrator.....	75
Delegate administrator permissions.....	76
Types of administrator permissions.....	76
Assigning, modifying, and removing administrator permissions on groups (Task Focused UI).....	79
Assigning administrator permissions (Standard UI).....	80
Modifying administrator permissions (Standard UI).....	80
Revoking administrator permissions (Standard UI).....	80
LDAP and user provisioning.....	81
Importing an LDAP certificate to the local trust store	81
Configuring LDAP access for user provisioning (Task Focused UI).....	81
Configuring LDAP access for user provisioning (Standard UI).....	82
Provisioning users.....	83
Creating user accounts (Task Focused UI).....	83
Creating user accounts (Standard UI).....	84
Modifying user accounts.....	86
Copying access from one user to another.....	87
Creating an organizational group (Task Focused UI).....	88
Associating and disassociating a group (Task Focused UI).....	89
Creating an organizational group (Standard UI).....	89
Associating and disassociating a group (Standard UI).....	89
Defining application permissions.....	90
Setting group application permissions.....	90
Types of application permissions.....	91
Application permissions not contained under the SOX heading.....	97
Configure password requirements.....	99
Configuring password policies.....	99
Updating the password encryption algorithm.....	99

Chapter 5. Security.....	105
Role-based security model.....	105
Security context points.....	107
Extending security context points.....	108
Security domains.....	110
Moving business entities.....	111
Copying business entities.....	111
Role-based access control permissions.....	111
Role templates.....	113
Accessing Role Templates.....	113
Adding a role template (Task Focused UI).....	114
Modifying a role template.....	115
Enabling and disabling a role template.....	115
Deleting a role template.....	116
Assigning and revoking roles.....	117
Assigning and removing a role from a user or group (Task Focused UI).....	117
Viewing roles assigned to users or groups.....	118
Adding a role template (Standard UI).....	118
Assigning a role to a user or group (Standard UI).....	119
Revoking a role from a user or group (Standard UI).....	120
Security rules.....	120
Record level security.....	121
Field level security.....	133
Paths for parent and child objects.....	136
Terms for data types.....	137
Grammar for security rules.....	139
Enabling or disabling a security rule.....	142
Validating a formula for a security rule.....	142
Deleting a security rule.....	143
Best practices for security rules.....	143
Custom security for projects.....	144
About the folder hierarchy and inheritance.....	144
Creating an Access Control List.....	145
Editing an Access Control List.....	145
Deleting an Access Control List.....	146
Encryption.....	146
Create a keystore.....	146
Configure a custom encryption key for passwords in properties files.....	148
Configure field level encryption.....	152
Updating the encryption keystore.....	153
LDAP user authentication.....	154
Configuring the LDAP Authentication Module.....	155
Setting up mixed-mode authentication.....	157
Configuring a multi-forested LDAP authentication.....	158
 Chapter 6. Managing the reporting schema	 159
Changes that require the reporting schema to be updated or recreated.....	159
Populating past reporting periods.....	160
Reporting schema permissions.....	161
Creating or recreating the reporting schema (Task Focused UI).....	162
Updating the reporting schema.....	162
Accessing the reporting schema (Standard UI).....	163
Creating or recreating the reporting schema (Standard UI).....	163
Enabling and disabling the reporting schema (Standard UI).....	163
Viewing reporting schema operation details (Standard UI).....	164
Generating the reporting schema and framework from a command line.....	164

Chapter 7. Managing reports.....	167
OpenPages with Watson V6 folder reports.....	167
Running reports (Task Focused UI).....	171
Running reports (Standard UI).....	171
Adding reports to OpenPages with Watson.....	171
Method 1: Using the Task Focused UI to add and edit reports.....	172
Understanding reports.....	172
Locating report files.....	172
Accessing report pages and page templates (Task Focused UI).....	173
Manually creating an instance of a report in the (Task Focused UI).....	173
Manually creating an instance of a Cognos dashboard or story (Task Focused UI).....	177
Method 2: Using the Standard UI to add reports.....	179
Report publishing limitations in the Standard UI.....	180
Accessing the publish report page (Standard UI).....	180
Publishing a report (Standard UI).....	180
Modifying the displayed report name or description.....	181
Creating an interactive JSP report (Task Focused UI).....	181
Running an interactive JSP report (Standard UI).....	182
Restricting access to reports in the Task Focused UI.....	182
Setting permissions on JSP and reports in the Task Focused UI.....	182
Securing access to the report portal.....	183
Chapter 8. System file management.....	187
System file management tasks	191
Managing system files and folders (Task Focused UI)	191
Creating folders (Standard UI).....	193
Uploading files (Standard UI).....	193
Moving files or folders (Standard UI).....	194
Copying files and folders (Standard UI).....	194
Renaming files or folders (Standard UI).....	194
Deleting files or folders (Standard UI).....	195
System file modification.....	195
Adding and modifying system files (Task Focused UI).....	195
Downloading files (Standard UI).....	196
Checking out files (Standard UI).....	197
Uploading modified files (Standard UI).....	197
Checking in files (Standard UI).....	197
Refreshing trigger configurations.....	198
Chapter 9. Fields and field groups.....	199
Definition of fields.....	199
Definition of a field group that is in use.....	199
Requirements for new fields.....	200
Field naming guidelines.....	201
Running the Schema Analysis report.....	202
Data types.....	203
Defining field groups.....	206
Adding field groups to object types.....	207
Defining fields and adding them to field groups.....	207
Making fields required or optional.....	209
Encrypting field values.....	209
Decrypting field values.....	210
Setting a default value for an object field.....	210
Defining boolean fields	211
Defining business entity selector fields	211
Defining a classifier field.....	212

Defining currency fields.....	212
Modifying currency exchange rates.....	213
Defining a date field	215
Defining decimal fields.....	216
Defining enumerated string fields.....	216
Defining integer fields.....	217
Defining long string fields.....	217
Defining simple string fields.....	218
Defining user/group fields.....	219
Field and field group process overview (Standard UI).....	221
Adding field groups (Standard UI).....	223
Adding fields to a field group (Standard UI).....	223
Modifying field group properties (Standard UI).....	224
Modifying object field definitions (Standard UI).....	224
Deleting field groups (Standard UI).....	225
Deleting an object field definition (Standard UI).....	225
Creating computed fields (Standard UI).....	225
Modeling a new computed field in Cognos	226
Defining a computed field.....	227
Using computed fields with multiple namespaces.....	229
Nesting computed fields.....	229
Troubleshooting: Computed fields validation.....	230
Troubleshooting: Computed field equation length limitation.....	230
Troubleshooting: Computed fields with cross products.....	230
Troubleshooting: Optimizing report request performance.....	231
Troubleshooting: Computed field query direction performance.....	232
Adding enumerated string values (Standard UI).....	232
Defining a default value for an enumerated string value (Standard UI).....	233
Changing the order of enumerated string values (Standard UI).....	233
Hiding enumerated string values (Standard UI).....	234
Unhiding enumerated string values (Standard UI).....	234
Deleting enumerated string values (Standard UI).....	235
Adding a currency field to a field group (Standard UI).....	235
Editing currency field information (Standard UI).....	236
Viewing and editing a currency display type (Standard UI).....	236
Editing currency field values in individual accounts (Standard UI).....	236
Modifying currency exchange rates (Standard UI).....	237
Reporting fragment fields.....	238
Tasks for configuring reporting fragment fields.....	238
Planning considerations for reporting fragment fields.....	239
Fields requiring parameter information.....	239
Defining a reporting fragment field.....	240
Using object fields to launch JavaServer Pages and external URLs.....	244
Attributes in the URL configuration string.....	244
URL configuration string examples.....	246
Configuring application text.....	247
Adding a URL launcher field	248
Adding a URL launcher field to views.....	248

Chapter 10. Object types.....249

Platform object types.....	249
Solution schema visualizations	250
Using the solution schema visualization editor	250
Creating a solution schema visualization	252
Property rendering JSP files.....	252
Accessing object types.....	253
Working with object types (Task Focused UI).....	253

Editing object type properties.....	254
Including field groups for an object type (Standard UI).....	255
Disabling associations between object types.....	255
Enabling associations between object types.....	256
Configuring OpenPages to associate a large number of child objects.....	257
Object relationship types.....	258
Setting the relationship type.....	259
Configure the ability to create a draft copy of an Object (Standard UI).....	260
Creating a field group and field for a Save As Draft configuration.....	260
Configure the Save As Draft feature for new objects.....	261
Adding the field to the object type and profile to configure the Save As Draft function	261
Stand-alone object settings.....	262
Enabling the creation of stand-alone objects.....	262
Enabling the ability to associate objects.....	262
File type information.....	263
Adding a file type.....	263
Associating a file type with an object type.....	264
Removing a file type from an object type.....	264
Tasks required to set up custom forms.....	265
Adding an object type for a custom form.....	265
Deleting a custom object type.....	266
Associating a custom form from a parent object.....	266
Associating a custom form to a parent object.....	267
Tasks to define filters for an object type.....	267
Filter considerations.....	268
Limitations on special characters in filters for long string fields.....	269
Adding filters to object types (Task Focused UI).....	271
Adding filters to object types (Standard UI).....	273
Dependent field behavior.....	278
Adding and working with dependent fields (Task Focused UI).....	279
Adding dependent fields (Standard UI)	280
Copying controller conditions (Standard UI).....	282
Modifying controllers for a dependent field (Standard UI).....	282
Enabling and disabling field dependency behavior (Standard UI).....	283
Deleting dependent fields (Standard UI).....	284
Configuration settings for the Add New wizard.....	284
Controlling the availability of object types in the Add New wizard.....	286
Controlling the display of tabs with no fields in the Add New wizard.....	286
Controlling the ability to use a template object when using the Add New wizard.....	287
Controlling the default object type in the parent picker in the Add New wizard.....	288
Configuring dependent picklists.....	288
Adding and working with dependent picklists (Task Focused UI).....	289
Adding dependent picklists (Standard UI).....	290
Modifying picklist dependency behavior (Standard UI).....	292
Enabling and disabling picklist dependency (Standard UI).....	292
Deleting a dependent picklist (Standard UI).....	293
Excluding fields from a subsystem.....	293
Selecting the fields to exclude.....	293
Changing the subsystem for an excluded field.....	294
Removing excluded fields.....	295
Chapter 11. Profiles.....	297
Guidelines for working with profiles.....	297
Accessing profiles.....	298
Creating a profile (Task Focused UI).....	298
Creating a profile (Standard UI)	299
Setting a default or fallback profile.....	300

Editing a profile.....	300
Deleting a profile.....	301
Enabling a profile.....	301
Disabling a profile.....	301
Associating profiles to a user.....	302
Associating users and groups to a profile.....	302
Disassociating users and groups from a profile.....	304
Including object types in a profile.....	304
Removing object types from a profile.....	305
Adding reports to a profile.....	305
Including fields in an object type.....	306
Excluding fields from an object type.....	306
Setting a field in a profile to required or optional.....	307
Setting the display order of object types (Standard UI).....	308

Chapter 12. Managing the Home page, views for objects, and display types.....309

Home page.....	309
The layout of tabs on a Home page.....	310
Configuring tabs on the home page.....	311
Adding tabs for reports or dashboards.....	311
Setting the display order of tabs.....	312
Hiding and unhiding tabs.....	312
Deleting tabs.....	313
Configuring the My Work tab.....	313
Configuring predefined lists.....	314
Filtered lists on the My Work tab.....	314
Configuring reports.....	316
Removing items from the My Work tab.....	319
Configuring users' Dashboard tabs.....	319
Creating content for users' Dashboard tabs.....	320
Editing the content of users' Dashboard tabs.....	321
Exporting the configuration for a dashboard tab.....	322
Configure views for objects.....	322
Navigational Views.....	323
Object views.....	325
Association views.....	326
Creation views.....	327
Enabling a view.....	327
Disabling a view.....	328
Setting a default view.....	329
Setting the display order of fields in a view.....	329
Copying views for an object from one profile to one or more other profiles.....	330
Including and excluding fields in navigation and association views.....	332
Including object types on an overview page.....	333
Excluding object types from an overview page.....	334
Associating filters to Filtered List view and Grid view pages.....	334
Disassociating filters from Filtered List view and Grid view Pages.....	335
Creating a Grid view	335
Creating Activity Views.....	337
Creating a Creation view.....	343
Configuring fields in Detail and Activity views.....	344
Inserting section headings.....	346
Modifying section headings.....	346
Deleting section headings.....	347
Setting object fields as read-only or editable.....	347
Spanning table columns.....	347
Configuring the display type for reporting fragment fields (Standard UI).....	348

Configuring display types for simple string fields (Standard UI).....	349
Configuring rich text display types for simple strings (Standard UI).....	349
Configuring the Business Entity Selector display type for simple string fields (Standard UI).....	350
Configuring text and URL display types for simple strings (Standard UI).....	351
Configuring URL link names by using the rich text display type for simple strings (Standard UI)..	352
Configuring text area display types for simple strings (Standard UI).....	353
Configure user and group selectors display types for simple strings (Standard UI).....	353
Configuring display types for long string fields (Standard UI).....	358
Configuring the on demand display types for long string fields (Standard UI).....	359
Configuring text display types for medium long string fields (Standard UI).....	360
Configuring rich text display types for medium long string fields (Standard UI).....	360
Configuring a display type for enumerated strings (Standard UI).....	361

Chapter 13. Configuring the Task Focused UI.....363

Setting up the Task Focused UI.....	363
Comparing the Standard UI and the Task Focused UI.....	365
Home page, dashboard, and tabs in the Task Focused UI.....	367
Defining a dashboard for a profile.....	368
Adding a Search panel.....	370
Views in the Task Focused UI.....	370
Combining field types from the Standard UI and the Task Focused UI.....	372
Planning the Grid Views.....	373
Using a Grid View.....	373
Designing a Grid View.....	374
Planning the Creation Views.....	376
Using a Creation View.....	377
Designing a Creation View.....	377
Planning the Task Views.....	380
Using a Task View.....	381
Designing a Task View.....	382
Using the View Designer.....	385
Defining a Grid View.....	389
Defining Grid Views for bulk workflow actions.....	390
Defining a Creation View.....	391
Defining Creation Views for file object types.....	393
Defining a Task View.....	394
Defining Task Views for file object types.....	395
Displaying debug information.....	397
Creating a custom view from a system view.....	398
Editing JSON for a view definition.....	398
Adding general elements to a view.....	399
Adding a section.....	399
Arranging fields in columns.....	400
Adding inline guidance.....	400
Adding user guidance.....	402
Applying light formatting to text	403
Defining a Task View header.....	404
Applying alternate field labels.....	405
Defining default filters on Grid Views.....	406
Adding and configuring fields on views.....	407
Apply colors to enumerated field values.....	407
Apply colors to value ranges.....	408
Supported color palettes for field values.....	409
Displaying a URL launcher field as a button or link.....	410
Displaying a number field as a progress bar.....	410
Adding a classifier field that makes taxonomy suggestions	410
Adding a business entity selector field	412

Adding and configuring relationship fields on views.....	413
Adding a card layout.....	414
Adding a chart diagram.....	416
Adding a count	424
Adding a grid layout.....	425
Adding a tree diagram.....	429
Adding a classifier field that makes object association suggestions.....	430
Adding rules to relationship fields.....	432
Organizing relationship fields in tab groups.....	433
Adding actions to relationship fields.....	434
Adding an Associate action.....	434
Adding an Associate Primary Parent action.....	435
Adding an Add New action.....	435
Adding a Copy Recursive action.....	436
Adding a Delete action.....	438
Adding a Get Watson Suggestion action.....	438
Defining dynamic filters on actions in relationship fields.....	438
Configuring rules.....	439
Defining Editable and Read Only rules.....	440
Defining Visible and Hidden rules.....	441
Defining Required rules.....	442
Defining Greater than, Greater than or equal, Less than, Less than or equal, and Equal rules.....	443
Defining Minimum Length and Maximum Length rules.....	444
Defining Pattern rules.....	445
Controlling error severity on rules.....	445
Customizing the Primary menu.....	446
Changing the order of menu items.....	446
Adding object types to a submenu.....	448
Creating a new top-level menu item.....	449
Configuring a Net Promoter Score (NPS) survey.....	450
Exporting and importing dashboards	452
Themes.....	452
Defining custom themes.....	454

Chapter 14. Configuring GRC Calculations..... 457

Setting up GRC Calculations.....	457
Calculation fundamentals.....	458
GRC Calculations FAQs.....	461
Designing a calculation.....	463
Common calculation use cases	464
Managing calculation definitions.....	466
Defining a calculation.....	467
Expressions in GRC Calculations.....	471
Syntax rules for expressions.....	471
Tutorial: writing expressions.....	473
Working with lists.....	475
Object fields	477
System variables	478
Functions for string values	479
Functions for lists and numerical values.....	481
Functions for dates.....	483
Functions for currency values.....	485
If/then/else/endif statements.....	486
Running a calculation as an administrator.....	490
Testing and debugging a calculation.....	491
Customizing email notifications for GRC Calculations.....	492

Chapter 15. Configuring GRC Workflow	495
Setting up GRC Workflow.....	495
GRC Workflow fundamentals.....	496
Workflow definitions and workflow instances.....	496
How workflows are started.....	497
Types of users who interact with workflows	498
How users interact with workflows	499
System workflow fields.....	502
Using variables, functions, and fields	503
Interpreting and viewing due dates.....	505
Designing a workflow.....	505
Using the GRC Workflow Designer.....	508
Defining a workflow.....	513
Defining workflow properties	514
Workflow stages.....	519
Defining a standard stage.....	519
Defining an end stage.....	523
Workflow actions.....	526
Defining a workflow action.....	527
Defining a workflow action that creates objects.....	532
Defining a workflow action that runs a custom action	535
Defining a workflow action that locks or unlocks objects.....	537
Defining a workflow action that sets fields.....	539
Defining a workflow action that starts a workflow.....	542
Defining a workflow action that runs a calculation.....	544
Starting workflow instances in bulk.....	546
Managing workflow instances.....	547
Exporting and importing workflow definitions.....	548
Customizing email notifications for GRC Workflow	548
Reporting on information in workflow instances.....	550
 Chapter 16. Scheduler.....	 551
Managing jobs	551
Defining a custom job.....	553
Defining a job that runs a JSP report.....	554
Implementing a Java class for custom jobs	556
 Chapter 17. Localizing text.....	 559
Configuring client systems to display Asian characters.....	559
Language and locale support.....	560
Localizing object text.....	561
Modifying object text (Task Focused UI).....	561
Modifying display text for an object text (Standard UI).....	563
Modifying display text for object fields (Standard UI).....	563
Modifying display text for public filters (Standard UI).....	563
Localizing system fields.....	564
Localizing application text.....	564
Modifying application text (Task Focused UI).....	566
Modifying application text (Standard UI).....	567
Modifying the bucket heading format of the phonebook.....	567
Modifying the user name format.....	568
Modifying overview menu links.....	570
Modifying navigational view links.....	570
Defining messages and behavior on the login screens.....	571
Defining the Privacy and Acceptable Use menu items.....	574
The Custom folder.....	576

Adding new keys.....	576
Modifying custom keys.....	576
Chapter 18. Reporting periods, object resets, and rulesets.....	577
Active reporting periods and operational limitations	577
Reporting period interactions.....	578
Using System Admin Mode with reporting periods	579
Reporting period permissions and settings.....	579
Creating and finalizing a reporting period (Task Focused UI).....	579
Deleting a reporting period (Task Focused UI).....	580
Creating a reporting period (Standard UI).....	580
Creating a finalized reporting period (Standard UI).....	581
Working with the active reporting period (Standard UI).....	581
Reapplying the active reporting period to a business entity (Standard UI).....	582
Finalizing a reporting period for a specific business entity (Standard UI).....	583
Finalizing a reporting period (Standard UI).....	583
Object resets.....	583
Creating a ruleset.....	584
Sample ruleset.....	585
Ruleset tag library.....	586
Loading the ruleset.....	591
Performing the object reset.....	592
Starting the object reset (Task Focused UI).....	592
Starting the object reset (Standard UI).....	594
Refreshing the reporting database after the reset.....	595
Exporting rulesets to an XML file.....	595
Chapter 19. Viewing the Configuration and Settings page.....	597
Managing settings (Task Focused UI).....	597
Modifying settings (Standard UI).....	598
Paths for settings in data loader files.....	599
Applications folder settings.....	599
Modify the overview view cache capacity.....	599
Configure the browser cache.....	599
Display the accessibility link.....	600
Display or hide field guidance.....	600
Display or hide system generated field guidance.....	600
Disable the Add New wizard from various launch points.....	600
Configure file check-out.....	602
Configure the sort order of object list views by modification date.....	602
Modify the deletion interval for a reporting period.....	602
Show hidden settings.....	602
Specify the browsers that can access IBM OpenPages.....	603
User provisioning settings.....	603
Configure actor table page size.....	605
Actor selectors: Configure the bucket size of the phonebook.....	605
Actor selectors: Configure display columns in a selector dialog box.....	606
Actor selectors: Configure users and group selectors for search.....	607
Menus: Update administration menus.....	607
Menus: Modify the order of menus.....	607
Menus: Modify submenus.....	607
Menus: Show items on the Administration > Object Menu	608
Object auto-naming settings.....	609
Configure the format of object names.....	610
SOXDocument object auto-naming settings for duplicate file names.....	611
Environment migration settings.....	612
Report fragment settings.....	612

Set the mail server address.....	612
Optimize file uploads.....	613
Number of objects in listing pane.....	614
Set copy operations.....	614
Date field display format.....	616
Configuring large files for upload.....	617
Allow opening Microsoft Office files directly from OpenPages.....	617
Reviewing the Net Promoter Score (NPS) survey settings.....	619
Signature and lock settings.....	619
Object Reset settings.....	624
Home page settings.....	625
Filtered List View settings.....	628
Bulk move and rename setting.....	633
Custom settings.....	633
Creating a custom setting.....	634
Deleting a custom setting.....	634
Copying settings and folders	634
Common folder settings.....	635
Maximum rows in exchange rate upload file.....	635
Use legacy associate.....	635
Exclude characters from user names.....	635
Set the system security model.....	635
Disable access control on Role groups.....	636
Configure self-contained object types.....	636
Enable the CodeCogs Equation Editor in Rich Text fields.....	637
Platform folder settings.....	638
Enable custom REST service.....	638
Compare Environments tool settings.....	638
Set localization options.....	639
Configure primary associations.....	639
Configure the legacy move behavior.....	640
Configure the host setting.....	640
Cross-context sharing.....	641
Platform Reporting Framework folder settings.....	642
Reporting Schema folder settings.....	642
Security settings.....	644
User Preferences folder settings.....	648
Set alert notification behavior.....	648
Chapter 20. Configuring the global search feature.....	649
Setting up global search.....	649
Setting login information for the search server.....	650
Changing the login information for the search server.....	652
Using OPBackup and OPRestore when global search is enabled.....	653
Enabling and disabling global search.....	653
Enabling and disabling file attachment searching.....	654
Enabling attachment file types for global search.....	654
Customizing global search.....	655
Enabling or disabling object types or fields for global search.....	655
Example: customizing global search on initial enablement.....	656
Example: adding or removing object types and fields with an already-enabled global search.....	657
Changing the database connection information for the search server.....	658
Displaying a custom field in global search results.....	659
Global search settings.....	660
Unhiding the hidden global search settings.....	660
Setting the Query Path to the global search administration server.....	660
Setting the URL to the global search administration server.....	660

Setting the progress refresh interval.....	661
Setting the number of records to cache.....	661
Setting the polling interval.....	662
Setting the number of records to cache before sending to the server for indexing.....	662
Setting the Query Path to the Apache Solr server that handles Folder ACL indexing.....	663
Setting the language analyzer that is used by search.....	663
Setting the Query Path to the Apache Solr server that handles Folder ACL indexing.....	663
Setting the URL to the Apache Solr server that handles Folder ACL indexing.....	664
Setting the number of records inserted per batch.....	664
Setting the Query Path to the Apache Solr server that handles Folder ACL search requests.....	665
Setting the URL to the Apache Solr server that handles OpenPages search requests.....	665
Setting the number of attempts to fill the search results.....	665
Setting the number of search results records that are cached per user session.....	666
Setting the internal page size for search results.....	666
Setting the URL to the Apache Solr server that handles search requests.....	666
Setting a time limit to search before timing out.....	667
Setting an additional field in the search result set.....	667
Setting whether to allow compression.....	667
Setting the network connection request timeout.....	668
Setting whether to allow URL redirects.....	668
Setting the number of allowed connections from the platform.....	668
Setting the number of allowed connections.....	669
Setting the number of times a request is reattempted.....	669
Setting the socket timeout for indexing.....	669
Setting the socket timeout for searching.....	670
Setting the Apache Solr password.....	670
Setting the Apache Solr user ID.....	670
Setting the default number of search results to return per page.....	670
The global search properties file.....	671
Setting the error handling parameters for the indexer.....	671
Setting the maximum opsearchtool.jar heap size.....	672
Setting the maximum Apache Solr heap size.....	672
Setting the maximum opsearchtool.jar heap size during indexing.....	672
Setting the maximum text extraction heap size for indexing.....	673
Setting the text extractor timeout limit.....	673
Setting the maximum text to extract from file attachments for indexing.....	674
Setting the root path location for file attachment search.....	674
Global search FAQs.....	675

Chapter 21. Using IBM OpenPages with Watson utilities with Db2 databases..... 679

Db2 and the OpenPages with Watson backup and restore utilities.....	679
Email notification for backup jobs.....	679
Configuring backup job notification.....	680
Asynchronous background jobs and administrative functions.....	681
Enabling and disabling asynchronous background processes checking.....	682
The OPBackup utility.....	682
Backing up custom files.....	683
Running a live OpenPages with Watson backup.....	684
OpenPages with Watson backed-up content.....	684
The OPBackup log file.....	685
Configuring OPBackup to use GZIP.....	685
Enabling and disabling storage backup.....	685
The OpenPages with Watson restore utility on the Db2 database.....	686
Running the OPRestore command.....	686
OPRestore log files.....	687
Using the Cognos Backup utility.....	687
The OpenPages with Watson file storage directory.....	687

Running the OPCCBackup command.....	687
The OPCCBackup log file.....	688
Cognos backed-up content.....	688
Configuring OPCCBackup to use GZIP.....	688
Using the Cognos Restore utility.....	689
Running the OPCCRestore command.....	689
The OPCCRestore log file.....	690
Db2 database backup and restore for OpenPages.....	690
Restoring backed up production data in a new Db2 environment.....	692
Refreshing a test environment from backup files (Db2).....	694
Prerequisites to refreshing a Db2 test environment.....	694
Backup of production databases in OpenPages with Watson on the Db2 server	694
Backing up and copying OpenPages with Watson application production files for a Db2 database.....	694
Backup of OpenPages with Watson databases on the test server.....	694
Backing up OpenPages with Watson application files on your test server.....	695
Running the OPCCBackup command.....	695
Drop the Db2 database for the application on the test system.....	695
Copy and restore the production Db2 database backup file to the test Db2 database server.....	696
Update the OpenPages with Watson storage location in the Db2 database.....	696
Back up the Cognos database on the Db2 production and test servers.....	698
Back up Cognos configuration files on the Db2 production and test servers.....	698
Modify SSO and LDAP configuration in the test environment.....	698
Copy and restore the Cognos production database backup file to the test database server.....	698
Drop the Db2 database for Cognos on the Test Server.....	699
Copy custom deliverables to the test environment.....	699
Copy custom triggers	699
Copy other custom deliverables to the test environment.....	700
Starting the OpenPages with Watson in the test environment.....	700
Updating the OPSys password.....	700
Update Db2 database connection references for Cognos	700
Update URL host pointers for Cognos reports.....	701
Update the global search settings.....	701
Utilities for filtering on long string field content in a Db2 database.....	702
Enable Db2 text search.....	702
Create a long string index in a Db2 database.....	703
Change the scheduled job that synchronizes the long string index in the database (Db2).....	705
Drop a long string index.....	707
Entity Move/Rename utility.....	708
Entity Move/Rename utility prerequisites.....	709
Configuring the Entity Move/Rename utility for a Db2 database.....	709
Prepare the input file for the Entity Move/Rename utility.....	710
Running the Entity Move/Rename utility interactively for a Db2 database.....	711
Running the Entity Move/Rename utility as a scheduled task.....	712
Impact of the Entity Move/Rename utility on the OpenPages application.....	712

Chapter 22. Using IBM OpenPages with Watson utilities with Oracle databases.. 713

Oracle databases and the backup and restore utilities.....	713
Prerequisite: Oracle client software.....	713
Oracle Data Pump.....	713
Email notification for backup jobs.....	714
Configuring backup job notification.....	714
Asynchronous background jobs and administrative functions.....	715
Enabling and disabling asynchronous background processes checking.....	716
Encrypting database passwords in the backup-restore utility environment files.....	717
The OPBackup utility.....	718
Modifying the backup-restore environment file.....	718

Backing up custom files.....	719
Running the OPBackup command.....	719
Backing up the OpenPages database (Oracle).....	720
Running a live OpenPages with Watson backup.....	721
OpenPages with Watson backed-up content.....	722
Enabling and disabling storage backup.....	722
The OpenPages restore utility on the Oracle database.....	723
Running the OPRestore command.....	723
OPRestore log files.....	724
Using the Cognos backup utility.....	724
Oracle Data Pump configuration on a first time use.....	725
The OpenPages with Watson file storage directory.....	725
Configuring or updating the Oracle Data Pump directory.....	725
Running the OPCCBackup command.....	726
The OPCCBackup log file.....	727
Cognos backed-up content.....	727
Configuring OPCCBackup to use GZIP.....	727
Using the Cognos restore utility.....	727
Running the OPCCRestore command.....	728
The OPCCRestore log file.....	728
Using Oracle online database backup (RMAN) for point-in-time recovery.....	728
Oracle online database backups.....	729
Running Oracle online database backups (RMAN).....	729
Monitoring the size of the Oracle backup area.....	734
Adjusting the size of the Oracle backup area.....	734
Disabling online backup of the Oracle database instance.....	736
Performing Oracle online database crash recoveries.....	736
Refreshing a test environment from backup files.....	736
Backing up and copying the OpenPages with Watson application production files for an Oracle database.....	737
Backing up the OpenPages with Watson application test files on your Oracle test data.....	737
Deleting data on the test database system.....	737
Copy the production database dump (.dmp) file to the test database server.....	737
Import the production data into the test environment.....	738
Update the OpenPages with Watson storage location in the Oracle database.....	739
Update the global search settings.....	741
Update Cognos data in the test environment.....	742
Modify SSO and LDAP Configuration in the test environment.....	745
Copy custom triggers	745
Copy other custom deliverables to the test environment.....	746
Starting the OpenPages with Watson in the test environment.....	746
Updating the OPSystem password.....	746
Update URL host pointers for Cognos reports.....	746
Utilities for filtering on long string field content in an Oracle database.....	746
Create a long string index for an Oracle database.....	747
Enabling Oracle Text.....	748
Create a schedule job to synchronize a long string index.....	749
Drop a long string index.....	750
Modifying the list of stop words.....	751
String concatenation utility.....	752
Running string concatenation.....	752
The string concatenation SQL file.....	754
Entity Move/Rename utility.....	758
Entity Move/Rename utility prerequisites.....	758
Configuring the Entity Move/Rename utility for an Oracle database.....	758
Prepare the input file for the Entity Move/Rename utility.....	759
Running the entity move/rename utility interactively.....	761
Running the Entity Move/Rename utility as a scheduled task.....	762

Impact of the Entity Move/Rename utility on the OpenPages application.....	762

Chapter 23. System Maintenance..... 763

Application server restrictions.....	763
Port assignments.....	763
Change default port numbers.....	764
Checking port number availability.....	764
Changing OpenPages with Watson application ports for an WebSphere Liberty environment.....	765
Updating port values in the database.....	767
Updating port values on the reporting server.....	767
Changing the OpenPages with Watson Framework Generation port.....	768
Updating URL host pointers for reports.....	769
Auditing configuration changes.....	770
Accessing the Configuration Audit Report.....	770
The Configuration Audit Report.....	771
Changing the password of the WebSphere Liberty keystore.....	771
Changing the keystore that is used by WebSphere Liberty.....	772
Changing the keystore that is used by Db2.....	773
Changing the OPSysm password.....	773
Changing database password references.....	774
Change database password references on the OpenPages with Watson application server.....	775
Modifying the OpenPages database password in Cognos	776
Modifying database passwords in the backup-restore environment files (Oracle only).....	776
Updating the Oracle Enterprise Manager tool.....	777
Changing database references.....	778
Testing the connection to the OpenPages database from the Oracle database client.....	778
Modifying the data source connection URL.....	779
Modify database references in the application configuration files.....	779
Modify database connection references for the reporting server.....	781
TLS for OpenPages with Watson environments.....	782
Accessing the OpenPages with Watson application using TLS.....	783
Verifying TLS ports on application servers.....	783
Generating a Certificate Signing Request file.....	783
Importing signed CA certificates.....	783
Importing the CA certificate for the Java Runtime Environment of Cognos Analytics.....	785
Installing CA certificates for all client browsers.....	785
Updating properties files so web browsers use the HTTPS protocol and TLS ports.....	786
Enabling secure session cookies on WebSphere Liberty.....	786
TLS configuration for Microsoft Internet Information Services.....	787
TLS configuration for Apache Web Server.....	789
TLS configuration on a Linux load balancer server	791
TLS configuration for CommandCenter for an Apache load balancer server (Windows).....	794
TLS configuration for Cognos for IBM HTTP Server	796
Configuring Cognos to connect to OpenPages by using TLS.....	798
TLS configuration for Db2.....	799
Modifying the LDAP configuration file for LDAP over TLS.....	802
Renewing TLS certificates for OpenPages with Watson.....	804
Setting up a secure connection for the global search service.....	806
Enabling a TLS database connection between the search server and the database server.....	809
Disabling the TLS database connection between the search server and the database server.....	810
Oracle Transparent Data Encryption (TDE).....	810
Prerequisites and process overview.....	810
Encrypting OpenPages and Cognos table spaces.....	811
Shortening the URL for OpenPages with Watson.....	815
Parameters for cluster members.....	816
Configuring HTTP compression in OpenPages with Watson	817
Enabling or disabling HTTP compression on OpenPages with Watson Application Servers.....	818

Enabling or disabling compression on the Cognos Server using Windows IIS.....	818
Enabling compression on the Cognos Server using Apache Web Server.....	818
Disabling compression on the Cognos Server using Apache Web Server.....	819
Factors that affect performance of activity and grid views.....	820
Server tuning settings.....	821
Changing JVM options on application servers.....	821
Configuring the reporting server.....	821
Configuring the database (Db2).....	822
Improve the performance of OpenPages application functions on a Db2 server.....	824
Installing tools and utilities (IBM OpenPages with Watson).....	824
Using log files.....	825
Configuring extended access logging on WebSphere Liberty.....	825
Collect log files and diagnostic data.....	826
OpenPages with Watson Standard Application Server log files (8.2.0.3 and earlier).....	828
OpenPages with Watson standard log files (8.2.0.4 and later).....	831
Troubleshooting browser issues.....	836
Optimizing application performance in Microsoft Edge browsers.....	836
Setting a session inactivity timeout value.....	836
Setting the Cognos Application Firewall for browser security.....	838
Browser security issues and running reports.....	839
Browser locale settings and messaging issues.....	839
Browser errors about Content Security Policy.....	839
Browser best practices.....	839
Chapter 24. Starting and stopping servers.....	841
Starting application servers.....	841
Starting application servers by using Windows services.....	841
Starting all application services by running a script (Windows).....	842
Starting all application servers by running a script (Linux).....	842
Determining application readiness.....	843
Stopping application servers.....	843
Stopping application servers by using Windows services.....	843
Stopping all application servers in Windows by using a script.....	843
Stopping all application servers on Linux by using a script.....	844
Start or stop the global search services.....	844
Starting the global search services by using a script.....	844
Stopping the global search services by using a script.....	845
Starting the global search services on Windows.....	845
Starting the global search services on Linux.....	846
Stopping the global search services.....	847
Start or stop the database services.....	847
Starting and stopping the Oracle database server in a Windows environment.....	848
Starting and stopping the Oracle database server in Linux environments.....	848
Starting and stopping the Cognos services.....	849
Using the IBM Cognos configuration tool to start and stop the IBM Cognos service.....	849
Using the Windows operating system to start and stop the IBM Cognos service.....	849
Using the Linux operating system to start and stop the IBM Cognos service.....	850
Starting and stopping the OpenPages with Watson Framework Model Generator service on Windows.....	850
Starting and stopping the OpenPages with Watson Framework Model Generator service on Linux.....	850
Chapter 25. Comparing IBM OpenPages with Watson environments.....	853
Review configuration settings.....	855
Supported items.....	856
Prepare the files to compare.....	856
Preparing files by using Export Configuration.....	857

Preparing files by using ObjectManager.....	857
Comparing environments.....	859
Interpret results.....	859
Errors, warnings, and how to fix them.....	861
Example: A field group exists in the source environment, but not in the target.....	861
Example: A profile exists in the target environment, but not in the source.....	863
Example: A custom object type exists in the target environment, but not in the source.....	863
Log files for the Compare Environments tool.....	864
Chapter 26. Migrating OpenPages environments.....	865
Settings that apply to environment migration.....	865
Supported migration items.....	866
Exporting dependencies.....	868
Items that are not migrated.....	869
Item dependencies not migrated by default.....	871
Environment migration best practices.....	872
The environment migration process.....	872
Exporting configuration items from the source environment (Task Focused UI).....	873
Exporting configuration items from the source environment (Standard UI).....	874
Importing configuration items to the target environment.....	875
Configuring environment migration to allow special characters.....	875
Validating a migration file.....	876
Importing a migration file (Task Focused UI).....	877
Importing a migration file (Standard UI).....	878
Chapter 27. Using ObjectManager.....	881
Working with loader files.....	881
Creating a data loader file.....	882
Running ObjectManager commands.....	882
ObjectManager command line parameters.....	883
Load command example.....	884
Dump command example.....	885
Batch loader file syntax and sample.....	885
Using ObjectManager to move objects.....	886
Using ObjectManager to rename objects.....	887
Using ObjectManager to assign or revoke role assignments.....	889
Using ObjectManager to create or load users.....	891
Modifying the ObjectManager properties file.....	892
Settings in the ObjectManager.properties file	893
Filtering data for export.....	898
Before you begin.....	899
About the filters configuration file.....	899
ObjectManager predefined filters.....	899
Sample filter configuration file.....	901
Controlling data load behavior.....	901
Managing currency exchange rates.....	902
Importing exchange rates.....	902
Exporting all currency exchange rates.....	903
Enabling and disabling currencies.....	903
Importing currency field definitions.....	904
Exporting currency field definitions.....	905
Importing computed field definitions.....	905
Exporting computed field definitions.....	906
Exporting file attachments.....	907
Migrating configuration changes using the ObjectManager tool.....	907
The ObjectManager migration process.....	908
Modifying ObjectManager settings.....	909

Migrating configuration changes.....	911
Chapter 28. Using FastMap	915
FastMap overview.....	915
The FastMap import process.....	916
FastMap templates.....	916
The FastMap data validation process.....	917
FastMap localization.....	917
FastMap can be accessed in both user interfaces.....	918
Accessing FastMap to import data and view status (Task Focused UI).....	918
Accessing FastMap to import data and view status (Standard UI)	919
Importing a FastMap data load template (Standard UI)	919
Resolving FastMap validation errors.....	920
Understanding FastMap validation errors.....	920
Troubleshooting FastMap conflict with recent updates warning message.....	921
Troubleshooting FastMap validation messages.....	921
Viewing FastMap import status.....	925
Using the FastMap import status report window (Standard UI).....	926
Understanding import status messages.....	926
Creating FastMap import templates.....	927
The data exported to a workbook by FastMap.....	927
Working with data load worksheets.....	928
Defining paths for objects.....	928
Using special column headings.....	929
Defining property fields for objects in FastMap templates.....	930
Guidelines for entering object data into FastMap templates.....	930
Adding custom columns and worksheets to FastMap templates.....	932
Sample Object worksheet for updating and creating objects.....	932
Sample self-contained object worksheet.....	933
Sample Business Entity worksheet for creating a new business entity structure.....	934
Using the FastMap Definition worksheet.....	934
Unhiding a FastMap Definition worksheet.....	935
FastMap parameters.....	935
FastMap export templates.....	935
Modifying parameters in the default FastMap export template (Standard UI).....	935
Modifying parameters in the default FastMap export template (Task Focused UI).....	936
Specifying a FastMap export template.....	936
FastMap parameters for importing and exporting data.....	937
Configuring a lookup key for FastMap	945
Modifying export settings to optimize FastMap performance.....	947
Limiting the rows for import to optimize FastMap performance.....	947
Setting a transaction timeout to optimize FastMap performance.....	948
Adding a processing delay to optimize FastMap performance.....	948
Securing FastMap import templates stored on the server.....	948
Cleaning up FastMap import templates stored on the server.....	949
AFCON-generated FastMap template best practices.....	949
Using FastMap with questionnaire template and assessment objects.....	950
Chapter 29. Configuring and generating the reporting framework.....	951
The reporting framework	951
Framework models.....	951
Namespaces	952
Facts and dimensions.....	953
Recursive object levels.....	953
Triangle object relationships.....	955
Object type dimensions.....	956
Planning the configuration.....	956

Configuring settings that apply to all framework models.....	957
Configuring the number of models that can be concurrently generated.....	957
Configuring reporting framework fact types.....	957
Including workflow fields	958
Adding locale codes to the reporting framework	958
Defining the sort order locale	959
Setting the triangle reporting framework object relationships.....	959
Enabling the reporting framework for custom forms.....	960
Defining the transaction timeout for reporting framework generation.....	960
Configuring framework models	961
Creating a framework model and namespace using a template	961
Defining a name for a framework model.....	961
Defining the format for a framework model.....	962
Enabling a framework model	962
Defining the query mode for a framework model	962
Defining the package label for a framework model	962
Defining whether a framework model uses profile filtering.....	963
Configure reporting framework namespaces.....	963
Defining a name for a reporting framework namespace.....	963
Defining the object model for a namespace	964
Setting a namespace as the default	965
Enabling a namespace.....	965
Defining entity recursive object levels for a namespace.....	965
Defining whether facts and dimensions are enabled for a namespace	965
Configuring facts and dimensions.....	966
Enabling and disabling facts.....	966
Enabling and disabling enumeration and dependent picklist dimensions.....	967
Using date dimension types.....	968
Configuring business entity recursive object levels.....	970
Defining business entity recursive object levels.....	970
Deleting business entity sets of recursive object levels.....	971
Modifying recursive object levels.....	972
Configuring object type dimensions.....	972
Adding object type dimensions.....	972
Modifying object type dimensions.....	973
Enabling, disabling, and deleting object type dimensions.....	974
Generating the reporting framework	974
Reporting framework permissions.....	975
Choosing update options in the reporting framework.....	976
Updating the reporting framework (Task Focused UI).....	977
Viewing reporting framework details (Task Focused UI).....	977
Accessing the reporting framework (Standard UI).....	977
Updating the reporting framework (Standard UI).....	978
Viewing reporting framework operation details (Standard UI).....	978

Chapter 30. IBM OpenPages with Watson connectors..... 981

IBM QRadar integration.....	981
Using the QRadar integration project.....	982
Configuring email notifications to be sent from the QRadar assembly line connector components.....	982
Specifying a primary parent ID to the OpenPages connector.....	983
Specifying currency values to the OpenPages connector by the output mapping.....	986
Specifying date values to the OpenPages connector via the output mapping.....	986
IBM OpenPages SDI Connector for UCF Common Controls Hub integration.....	986
Run the UCF assembly lines.....	987
IBM Security Directory Integrator (SDI) techniques.....	988
Scheduling Security Directory Integrator.....	988

Security Directory Integrator command line tips.....	988
Troubleshooting the assembly line "Connection refused" error.....	989
Chapter 31. Configuring questionnaire assessments	991
Configuring questionnaire assessments.....	991
Chapter 32. Configuring timesheet helpers for auditors.....	993
Chapter 33. Configuring the approval app.....	995
Configuring the JSON file for the approval app	995
Approval app certification questions.....	999
Customizing the JSON file for the approval app	1001
Chapter 34. Configuring OpenPages Loss Event Entry.....	1003
Planning the configuration	1003
How users are handled.....	1005
Where loss events get created.....	1005
Who loss events get assigned to	1005
How dates are validated.....	1006
How to launch OpenPages Loss Event Entry	1006
How confirmation emails are configured.....	1009
Using the Loss Event Entry Configuration tool.....	1010
Chapter 35. Configuring IBM Watson Integrations.....	1013
IBM Watson Assistant	1013
Configuring a web chat assistant by using IBM Watson Assistant.....	1013
Configuring the integration between an assistant and OpenPages	1014
Enabling additional security features for IBM Watson Assistant on IBM Cloud.....	1016
IBM Watson Language Translator.....	1018
Configuring IBM Watson Language Translator on IBM Cloud.....	1020
Configuring the integration between IBM Watson Language Translator and OpenPages	1020
Natural language processing services	1021
Configuration overview for natural language classifier services.....	1023
Configuring Watson Discovery	1025
Configuring a Natural Language Understanding service on IBM Cloud.....	1025
Configuring a Natural Language Classifier on IBM Cloud.....	1026
Defining a Classifier Configuration (Task Focused UI).....	1028
Defining a Classifier Configuration (Standard UI).....	1029
Defining a classifier field.....	1030
Monitoring and downloading classifier data usage	1031
Importing a Watson certificate to the local truststore	1031
Chapter 36. IBM OpenPages Data Privacy Management.....	1033
Installing IBM OpenPages Data Privacy Management.....	1034
Installing DPM on IBM OpenPages for IBM Cloud Pak for Data.....	1034
Installing DPM on IBM OpenPages with Watson.....	1034
Importing a certificate for Watson Knowledge Catalog into the local trust store	1035
Configuring the Watson Knowledge Catalog connector.....	1036
Chapter 37. Configuring IBM OpenPages Regulatory Compliance Management..	1039
Ascent Connector.....	1039
Importing a certificate for Ascent into the local trust store	1039
Configuring the Ascent connector.....	1040
Reloading Ascent data.....	1041
Thomson Reuters Connector.....	1041
Preparing the SFTP server.....	1042

Configuring the feeds.....	1043
Importing a certificate for Thomson Reuters into the local trust store	1043
Configuring the Thomson Reuters import.....	1044
Thomson Reuters taxonomy mapping.....	1046
Reg-Track Connector.....	1049
Importing a certificate for Reg-Track into the local trust store	1049
Configuring the Reg-Track connector.....	1050
Reg-Track taxonomy mapping.....	1051
Wolters Kluwer Connector.....	1054
Importing a certificate from Wolters Kluwer to the local trust store	1055
Configuring the Wolters Kluwer import.....	1055
Wolters Kluwer taxonomy mapping.....	1057
Processing regulatory events by using rules.....	1060
Creating rules.....	1060
Copying a rule.....	1063
Enabling and disabling rules.....	1064
Editing rules.....	1064
RCM Theme Deployer.....	1065
Process overview for the RCM Theme Deployer.....	1065
Installing the RCM Theme Deployer.....	1066
Configuring the RCM profile.....	1067
Setting up auto-naming for RCM objects.....	1067
Using the RCM configuration tool.....	1068
Chapter 38. Configuring IBM OpenPages Third Party Risk Management.....	1071
SecurityScorecard connector for IBM OpenPages Third Party Risk Management.....	1071
Importing a certificate for SecurityScorecard into the local trust store	1071
Configuring the SecurityScorecard connector.....	1072
Supply Wisdom connector for IBM OpenPages Third Party Risk Management.....	1073
Importing a certificate for Supply Wisdom into the local trust store	1073
Configuring the Supply Wisdom connector.....	1074
Appendix A. The Notification Manager.....	1075
The notification reports.....	1075
Results of running a notification report.....	1075
Requirements for setting up a notification.....	1075
Setting up a notification.....	1076
Task 1: Creating a page template	1076
Task 2: Creating the notification.....	1076
Task 3: Triggering the notification.....	1077
Appendix B. Properties and parameters.....	1081
Aurora properties and parameters.....	1081
OpenPages server properties and parameters.....	1083
Sosa properties and parameters	1084
Tools properties and parameters	1085
Appendix C. Non-role based access control.....	1087
Using ACLs with top-level folders.....	1087
The object folder structure.....	1087
Using inheritance with Access Control Lists.....	1088
Breaking inheritance.....	1088
Creating an ACL on a folder.....	1089
Editing an existing ACL.....	1089
Deleting an existing ACL.....	1090
Using groups to establish user roles.....	1090
The core IBM OpenPages Governance Platform 5.1x (and earlier) groups.....	1090

Example: Using groups to establish user roles.....	1091
Using groups to limit user activities.....	1091
Using nested groups to limit user scope.....	1093
Limiting user access by breaking folder inheritance.....	1093
Limiting user access by nesting user groups.....	1093
Limiting user access by setting folder Access Control Lists.....	1094
Using group ACLs to traverse business entities.....	1095
Appendix D. Troubleshooting and support	1097
Techniques for troubleshooting problems.....	1097
Searching knowledge bases.....	1098
Getting fixes.....	1099
Contacting IBM Support.....	1099
Exchanging information with IBM.....	1100
Sending information to IBM Support.....	1101
Receiving information from IBM Support.....	1101
Subscribing to Support notifications.....	1101
Known problems and solutions for global search.....	1102
Global search start fails.....	1102
Global search setup fails.....	1102
Forcing a reset of global search.....	1103
Checking for global search setup issues and periodic monitoring.....	1104
Before you contact IBM OpenPages Support.....	1105
QRadar integration package.....	1105
SDI properties file error message.....	1105
Do not include security domain groups when creating object filters or security rule formulas.....	1106
Objects can be saved with an empty required field.....	1106
JSON file might not display multibyte characters correctly in Wordpad.....	1106
Remediating after an Enumerated String field is changed to a multi-select field (Db2).....	1106
System delay when modifying object types and fields (Db2).....	1107
NoClassDefFoundError errors when you run custom code.....	1108
Risk Assessment Summary report does not show related risks and controls.....	1108
Troubleshooting helpers.....	1108
Appendix E. Best practices for configuring IBM OpenPages with Watson	1109
Use short field names and field group names.....	1109
Be aware that Java applets are not supported by the Chrome browser.....	1109
Limit the number of objects in views.....	1109
Limit the number of associations in the Overview.....	1109
Limit the number of portlets on the home page.....	1110
Limit activity views with field dependencies and dependent picklists.....	1110
Limit the number of security rules and complexity of security rules.....	1110
Limit the number of SOXBusEntity objects in the system.....	1111
Be aware of shared field groups.....	1111
Eliminating unused object type relationships.....	1111
Displaying reporting fragments only on demand.....	1112
Displaying Cognos reports on home page tabs.....	1112
Setting a minimal starting group for display types.....	1113
Task-oriented hyperlinking.....	1113
Appendix F. Creating custom actions for GRC workflows.....	1117
Appendix G. OpenPages API documentation.....	1121
Appendix H. Personal information processed and stored by OpenPages.....	1123

Notices.....	1125
Glossary.....	1129
Index.....	1131

Introduction

IBM OpenPages® with Watson™ is an integrated governance, risk, and compliance (GRC) platform that enables companies to manage risk and regulatory challenges across the enterprise.

Audience

The *IBM OpenPages with Watson Administrator's Guide* is intended for use with IBM OpenPages with Watson on-premises and on cloud. The content contains instructions for maintaining, configuring, and administering the OpenPages application. It is intended for use by administrators who have a background in systems management. Topics include user and group administration, database backup and restoration, customizing the application's look and feel, and using the data loader capabilities.

Please read the following important information regarding IBM OpenPages with Watson documentation

IBM® maintains one set of documentation serving both cloud and on-premises IBM OpenPages with Watson deployments. The IBM OpenPages with Watson documentation describes certain features and functions which may not be available on the cloud.

If you have any questions about the functionality available in the product version that you are using, contact IBM OpenPages Support by using the [IBM Support portal](#).

Finding information

To find product documentation on the web, including all translated documentation, access [IBM Documentation](#).

Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products. OpenPages documentation has accessibility features. PDF documents are supplemental and include no added accessibility features.

Forward-looking statements

This documentation describes the current functionality of the product. References to items that are not currently available may be included. No implication of any future availability should be inferred. Any such references are not a commitment, promise, or legal obligation to deliver any material, code, or functionality. The development, release, and timing of features or functionality remain at the sole discretion of IBM.

Database tool information

IBM OpenPages with Watson supports both the IBM Db2® database and the Oracle database. (Oracle is not supported in IBM OpenPages for IBM Cloud Pak for Data).

- To run OpenPages with Watson SQL scripts, you must use CLPPlus with Db2, and SQL*Plus with Oracle database.
- To run queries, you can use any SQL tool that is compatible with the database. For example, you could use CLPPlus or Optim™ Development Studio to run queries on the Db2 database.

IBM OpenPages with Watson

IBM OpenPages with Watson serves as the foundation for a company's enterprise risk management (ERM) efforts by unifying enterprise-wide risk and compliance initiatives into a single management system. With solutions for Financial Controls Management, Operational Risk Management, IT Governance, Policy Management, and Internal Audit, OpenPages with Watson provides a modular and integrated approach to governance, risk, and compliance.

Each component provides a highly configurable capability that supports your specific methodology, without having to write custom code, whether in loss events, KRI, or any other solution component. The result is that companies can embed risk management into the business and improve outcomes over time.

OpenPages with Watson solutions

The IBM OpenPages with Watson consists of the following solutions:

- IBM OpenPages Operational Risk Management (ORM) provides a fully integrated operational risk solution, including risk control self-assessments (RCSAs), key risk indicators, (KRIs), loss event data management, and advanced reporting and business intelligence with IBM Cognos® finance integrated risk management. Dashboard components are available to provide an enterprise-wide view of risk across the business and manage Basel II AMA compliance in the banking industry.
- IBM OpenPages Business Continuity Management (BCM) is used by an organization, or group, to maintain or resume a predetermined level of operations during or after a disruptive event. All risks that can potentially impact the business during or following an event are identified.
- IBM OpenPages Financial Controls Management (FCM) reduces the time and resource costs that are associated with ongoing compliance for financial reporting regulations.
- IBM OpenPages Model Risk Governance (MRG) supports organizations in organizing and centralizing their Model Inventory.
- IBM OpenPages Policy Management (PCM) provides an integrated solution for reducing the complexity of complying with numerous industrial, ethics, privacy, and government regulatory mandates.
- IBM OpenPages IT Governance (ITG) provides a risk-based, policy-driven approach to managing risk and compliance initiative for the IT organization.
- IBM OpenPages Internal Audit Management (IAM) provides an integrated audit management solution to manage the full life cycle of internal audits.
- IBM OpenPages Regulatory Compliance Management (RCM) supports organizations in breaking down regulations into a catalog of requirements, evaluating its impact to the business, and creating actionable tasks.
- IBM OpenPages Third Party Risk Management (TPRM) supports firms in assessing and analyzing risks that are associated with the vendors they do business with.

How IBM OpenPages with Watson can help

The OpenPages with Watson application provides many capabilities to simplify and centralize compliance and risk management activities.

Show me

This video provides an overview of OpenPages.

[OpenPages Overview](#)

This video provides an overview of AI in OpenPages.

[AI in OpenPages](#)

Shared content management and common repository

- Logically presents processes, risks and controls in many-to-many and shared relationships at multiple levels that can be configured to your business processes
- Supports importing existing corporate data and maintains a complete audit trail and version history
- Ensures consistent regulatory enforcement and monitoring across multiple regulations.

Dynamic decision support with Cognos

- Delivers rich, interactive, real-time executive dashboards and reports
- CrossTrack enables drill-down from reports into supporting reports as well as the underlying detail data
- Provide organizational assurance for regulatory compliance

Simple configuration and localization

- Detail user-specific tasks and actions on a personal home page.
- Reduce training costs with intuitive navigation, easy-to-use web-based layout and localized text in English (both UK and US), French, Italian, Spanish, German, Japanese, Simplified Chinese, Traditional Chinese, and Brazilian Portuguese.
- Lower administration costs with simple browser based configuration capabilities managed by administrators for end-users.

Flexible automation

- Streamlined compliance procedures and automated sub-certifications without sacrificing risk.

Web services-based integration

- OpenAccess API Interoperate with leading third-party applications to enhance policies and procedures with actual business data
- Reduced total cost of ownership and easy integration with existing corporate compliance management systems

Installation locations for IBM OpenPages with Watson

The installation directory is the location of product artifacts after a package, product, or component is installed. The following table lists the conventions that are used to refer to the installation location of installed components and products:

Important: Directory locations that contain spaces are not supported. IBM OpenPages with Watson or any software that is used by it must not be installed into a directory with spaces. For example, do not install database server, database client, or application server software into the Program Files directory.

If you're using IBM OpenPages for IBM Cloud Pak for Data, see the *IBM OpenPages with Watson Administrator's Guide*.

Table 1. Variable notations for installation directories

Directory	Description
<installation_server_home>	The directory where the IBM OpenPages with Watson installation server is installed. For example: • On Windows: C:\IBM\OPInstall\OP_<version>_Installer • On Linux®: /home/opuser/IBM/OPInstall/OP_<version>_Installer
<agent_home>	The directory where the IBM OpenPages with Watson installation agent is installed on a remote server. For example: • On Windows: C:\IBM\OPAgent • On Linux: /home/opuser/IBM/OPAgent
<OP_HOME>	The directory where OpenPages with Watson is installed. For example: • On Windows: C:\IBM\OpenPages • On Linux: /opt/opuser/IBM/OpenPages In the installation app, you specify the <OP_HOME> directory in the OP Home Directory field each Application Server card.
<ORACLE_HOME>	The installation location of the Oracle database software. For example: • On Windows: – C:\app\oracle\product\19.0.0\client_1 (Oracle Admin Client) – C:\oracle\instantclient_19_9 (Oracle Instant Client) – C:\app\oracle\product\19.0.0\dbhome_1 (server) • On Linux: – /home/oracle/app/oracle/product/19.0.0/client_1 (Oracle Admin Client) – /home/oracle/instantclient_19_9 (Oracle Instant Client) – /home/oracle/app/oracle/product/19.0.0/dbhome_1 (server)
<DB2_HOME>	The installation location of the IBM Db2 software. For example: • On Windows: C:\IBM\SQLLIB • On Linux: /home/db2inst1/sqllib

Table 1. Variable notations for installation directories (continued)

Directory	Description
<WLP_HOME>	The installation location of IBM WebSphere® Liberty. For example: • On Windows: <OP_HOME>\wlp • On Linux: <OP_HOME>/wlp
<WLP_USER_HOME>	The location of OpenPages with Watson application files and server configuration files. For example: • On Windows: <OP_HOME>\wlp-user • On Linux: <OP_HOME>/wlp-user
<COGNOS_HOME>	The installation location of Cognos Analytics. For example: • On Windows: C:\IBM\cognos\analytics • On Linux: /usr/IBM/cognos/analytics
<JAVA_HOME>	The installation location of IBM SDK, Java™ Technology Edition or Java Runtime Environment (JRE). IBM SDK example on an application server: • On Windows: C:\IBM\java_8.0_64 • On Linux: /opt/IBM/java_8.0_64 JRE example on a reporting server where Cognos Analytics is installed: • On Windows: C:\IBM\cognos\analytics\jre • On Linux: /usr/IBM/cognos/analytics/jre Note: In Cognos Analytics 11.1.5 and later, the path is: • On Windows: C:\IBM\cognos\analytics\ibm-jre\jre • On Linux: /usr/IBM/cognos/analytics/ibm-jre/jre IBM SDK example on a search server: • On Windows: C:\IBM\java_8.0_64\ • On Linux: /opt/IBM/java_8.0_64/
<CC_HOME>	The installation location of OpenPages with Watson CommandCenter. For example: • On Windows: C:\IBM\OpenPages\CommandCenter • On Linux: /opt/IBM/OpenPages/CommandCenter

Table 1. Variable notations for installation directories (continued)

Directory	Description
<SEARCH_HOME>	The installation location of global search. The <SEARCH_HOME> directory contains the opsearchtools.jar, Apache Solr, and other global search files. The global search indexing directory is also stored in the <SEARCH_HOME> directory. For example: • On Windows: C:\IBM\OpenPages\OPSearch • On Linux: /opt/IBM/OpenPages/OPSearch In the installation app, you specify the <SEARCH_HOME> directory in the Search Home Directory field on the Search Server card.

Special characters in passwords

You can use certain special characters in certain passwords.

If you are upgrading or migrating from 8.1.0.1 or earlier, install the 8.2 installation server, complete the upgrade or migration process, and then update passwords to use special characters.

The special characters that you can use in passwords are:

. + - [] * ~ _ # : ?

Note: Spaces are not supported.

You can use these special characters in database user passwords and operating system accounts for database schema owners.

If you use special characters in passwords, you must surround the password in quotation marks. Use the following syntax:

IBM Db2 connection strings

For Db2 databases, when you provide a password in a connection string, use the following syntax:

On Linux, use \ ' around the password. For example:

```
clpplus -nw openpage/\ 'DB~Password\ '@host:50000/opx
```

On Windows, use single quotation marks around the password:

```
clpplus -nw openpage/'DB~Password '@host:50000/opx
```

IBM Db2 script parameters in CLPPlus

For Db2 databases, when you provide a password in a script parameter, use the following syntax:

On Linux, use one of the following options:

- Use \ ' around the password. For example:

```
clpplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql  
/tmp/log.log c6de0652985e 50000 OPX db2inst1 \ 'DB~Password\ ' openpage
```

- Use \" around the password:

```
clpplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql  
/tmp/log.log c6de0652985e 50000 OPX db2inst1 \"DB~Password\" openpage
```

On Windows, use one of the following options:

- Use ' around the password. For example:

```
clppplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql
/tmp/log.log jwinpages.swg.usma.ibm.com 50000 OPX db2admin 'DB~Password' openpage
```

- Use \" around the password:

```
clppplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql
/tmp/log.log jwinpages.swg.usma.ibm.com 50000 OPX db2admin \"DB~Password\" openpage
```

Db2 utilities

When you run Db2 utilities, such as `db2 connect` or `db2rbind`, do not use quotation marks around passwords.

Oracle connection strings

For Oracle databases, when you provide a password in a connection string, use \" around the password. For example:

```
sqlplus sys/\"DB~Password\"@op as sysdba
```

Oracle script parameters in SQL*Plus

For Oracle databases, when you provide a password in a script parameter, use the following syntax:

- On Windows, use double quotation marks around the password.

```
sqlplus /nolog @sql-wrapper.sql
update-storage c:\temp\upd-storage-output.log
op openpages "pass-word" LFS eng11 eng11
Windows c:\OpenPages\openpages-storage
```

- On Linux, use single quotation marks around the password.

```
sqlplus /nolog @sql-wrapper.sql
update-storage /home/op/upd-storage-output.log
op openpages 'pass-word' LFS eng11 end11
Unix /usr/opdata/openpages-storage
```

Installation scripts, tools, and utilities

For tools and utilities that take the password as a parameter, use the following syntax:

- On Windows, use double quotation marks around the password.

```
op-validate-dba-install.bat "DB~Password"
```

- On Linux, use single quotation marks around the password.

```
./op-validate-dba-install.sh 'DB~Password'
```

Passwords in property files

For `.env` files and `.properties` files, do not use any quotation marks around passwords.

Variables and placeholders

When you run commands in IBM OpenPages with Watson, you need to know the values for various variables or placeholders.

For example, a command might require you to enter the `<server_name>` of an application server. The following table shows you how to find this value by looking in the `deploy.properties` file or in the installation app.

Table 2. Variables in commands (IBM OpenPages with Watson)

Parameter	Where to find it
<OP_HOME>	• In the <code>deploy.properties</code> file: in each <code>[app.server<N>]</code> section, <code>op_home_directory</code> • In the installation app: on each Application Server card, OP Home Directory
<server_name>	• In the <code>deploy.properties</code> file: in each <code>[app.server<N>]</code> section, <code>op_server_name</code> • In the installation app: Application ServerN card: OP Server Name When you reference an application server, you use the format <code><server_name>Server<N></code>. For example, suppose OP Server Name on the Application Server1 card is set to <code>opapp</code>. The full name of the admin application server is: <code>opappServer1</code>.

Chapter 1. What's new?

New and changed features affect the administration of IBM OpenPages with Watson.

For information about all new features for this release, see the *IBM OpenPages with Watson New Features Guide*.

For an up-to-date list of environments that are supported by OpenPages with Watson, see the [Supported Environments website](#).

New and changed features in version 8.2.0.4

New and changed features in version 8.2.0.4 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

IBM OpenPages for IBM Cloud Pak for Data

For more information, see [Chapter 2, “Administering IBM OpenPages for IBM Cloud Pak for Data,”](#) on page 33.

Platform enhancements

Table 3. Platform enhancements	
For information about...	See topic...
The  > Watson Integrations menu was renamed. It is now called  > Integrations	Chapter 35, “Configuring IBM Watson Integrations,” on page 1013
The  > Reporting Periods > Reporting Periods menu item is now  > System Configuration > Reporting Periods	Chapter 18, “Reporting periods, object resets, and rulesets,” on page 577
The  > Reporting Periods > Object Resets menu item is now  > System Configuration > Object Resets .	Chapter 18, “Reporting periods, object resets, and rulesets,” on page 577
The  > System Configuration > NPS Settings menu item is now  > Integrations > NPS Settings .	“Configuring a Net Promoter Score (NPS) survey” on page 450
The impact of the hyphen character (-) in display name format strings for user names has changed.	“Modifying the user name format” on page 568
The ability to enable or disable reports for profiles.	“Adding reports to a profile” on page 305
Integrating an IBM Watson Natural Language Understanding classifier into OpenPages	“Natural language processing services ” on page 1021
The Applications > GRCM > Object Move > Allow Hierarchical Moves setting now also controls rename operations.	“Bulk move and rename setting” on page 633

Administration and serviceability enhancements

Table 4. Administration and serviceability enhancements	
For information about...	See topic...
Logging with Apache Log4j 2	“OpenPages with Watson standard log files (8.2.0.4 and later)” on page 831
The ObjectManagerLogging.properties file has been removed. The logging for ObjectManager is now defined in the client tools' log4j2.properties file.	“OpenPages with Watson standard log files (8.2.0.4 and later)” on page 831
Generating the reporting schema and framework by using the RpsRpf command line tool	“Generating the reporting schema and framework from a command line” on page 164

New and changed features in version 8.2.0.3

New and changed features in version 8.2.0.3 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

IBM OpenPages for IBM Cloud Pak for Data

For more information, see [Chapter 2, “Administering IBM OpenPages for IBM Cloud Pak for Data,” on page 33](#).

Platform enhancements

Table 5. Platform enhancements	
For information about...	See topic...
The new API Version field on the configuration page for IBM Watson Language Translator	“Configuring the integration between IBM Watson Language Translator and OpenPages” on page 1020
The new application permission: Bulk Update All Fields	“Types of application permissions” on page 91

Solution enhancements

See the *IBM OpenPages with Watson Solutions Guide* for a complete list of all the changes to solutions.

Table 6. Solution enhancements	
For information about...	See topic...
OpenPages Third Party Risk Management includes a new connector to import data from Supply Wisdom	“Supply Wisdom connector for IBM OpenPages Third Party Risk Management” on page 1073
The new application permission: SupplyWisdom Feed	“Types of application permissions” on page 91

Administration and serviceability enhancements

Table 7. Administration and serviceability enhancements	
For information about...	See topic...
New application permissions for FastMap in the Task Focused UI	“Types of application permissions” on page 91

Task Focused UI

Table 8. Task Focused UI enhancements	
For information about...	See topic...
The ability to search for fields in Creation Views, Task Views, and Quick Views.	“Designing a Creation View” on page 377 , “Designing a Task View” on page 382
The FastMap import process	“The FastMap import process” on page 916 , “Accessing FastMap to import data and view status (Task Focused UI)” on page 918 , “Viewing FastMap import status” on page 925
The menu item for defining classifiers has changed to  > Watson Integrations > Mapping and Taxonomy Suggestions . It was previously named Administration > Cognitive Services > Natural Language Classifiers .	“Defining a Classifier Configuration (Task Focused UI)” on page 1028
IBM Watson Discovery was added as a natural language processing service.	“Natural language processing services ” on page 1021 “Configuring Watson Discovery ” on page 1025
The fields that are allowed to be updated by using Bulk Update () in Grid Views can now be configured.	“Designing a Grid View” on page 374 “Defining a Grid View” on page 389
It is now easier to create new views from existing ones. When creating new views in the View Designer, Copy from view (Optional) now allows you to copy from any existing published custom or system view (for the view type and object type).	“Defining a Creation View” on page 391 “Defining a Grid View” on page 389 “Defining a Task View” on page 394
Labels for existing fields can now be edited directly on the field definition.	“Defining fields and adding them to field groups” on page 207
Object type associations can now be enabled and disabled by using  > Solution Configuration > Objects Types .	“Enabling associations between object types” on page 256 “Disabling associations between object types” on page 255
The  > Solution Configuration > Objects menu item was renamed to  > Solution Configuration > Object Types .	

Table 8. Task Focused UI enhancements (continued)	
For information about...	See topic...
Reports can now be added to profiles. Users can now define report tabs on their dashboard. Previously, report tabs could be created only by administrators by using the Manage Dashboards task in the Task Focused UI.	“Adding reports to a profile” on page 305

GRC Workflow

Table 9. GRC Workflow enhancements	
For information about...	See topic...
Calculations can now be started directly from a workflow action. - Added Calculation Type to calculation definitions. Valid values are Automatic or Manual. Manual calculations are started only by a run a calculation action in a workflow. - Added the new run a calculation action to workflow stages.	“Defining a calculation” on page 467 “Defining a workflow action that runs a calculation” on page 544

New and changed features in version 8.2.0.2

New and changed features in version 8.2.0.2 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

IBM OpenPages for IBM Cloud Pak for Data

For more information, see [Chapter 2, “Administering IBM OpenPages for IBM Cloud Pak for Data,” on page 33](#).

Platform enhancements

Table 10. Platform enhancements	
For information about...	See topic...
The default value for the user name format application text (com.display.name.format) was changed to %FN; %LN; - %EM (first name, last name, email).	“Modifying the user name format” on page 568
The new setting Applications > GRCM > Allow Hierarchical Moves, which is set to false by default.	Controls whether child objects are moved with their parent objects by using the  icon in Grid Views: “Bulk move and rename setting” on page 633

Solution enhancements

See the *IBM OpenPages with Watson Solutions Guide* for a complete list of all the changes to solutions.

<i>Table 11. Solution enhancements</i>	
For information about...	See topic...
Configuring IBM OpenPages Data Privacy Management	Chapter 36, “IBM OpenPages Data Privacy Management,” on page 1033
When you regulatory library data from Thomson Reuters into IBM OpenPages Regulatory Compliance Management, mandates are now created.	“Thomson Reuters Connector” on page 1041

Administration and serviceability enhancements

<i>Table 12. Administration and serviceability enhancements</i>	
For information about...	See topic...
Improved logging for SAML, OIDC, and SPNEGO single sign-on	“Enabling trace logging” on page 829
Name changes Note the following changes: • <code>bcprov-jdk14-145.jar</code> is now <code>bcprov-jdk15to18-1.68.jar</code> • <code>org.bouncycastle145.jce.provider.BouncyCastleProvider</code> is now <code>org.bouncycastle.jce.provider.BouncyCastleProvider</code> • <code>CAMCryptoBC</code> is now <code>BC</code>	
Access to system files in the /Reports folder has changed. By default, only super administrators and members of the OPAdministrator group can now create or modify the JSP report system files in the /Reports folder under  > System Configuration > System Files .	“Adding and modifying system files (Task Focused UI)” on page 195

Task Focused UI

<i>Table 13. Task Focused UI enhancements</i>	
For information about...	See topic...
Defining themes.	“Themes” on page 452 “Types of application permissions” on page 91
Colors are now based on two Carbon color palettes, Categorical and Monochromatic.	“Supported color palettes for field values” on page 409
Applying a color palette when configuring enumerated fields in the View Designer.	“Apply colors to enumerated field values” on page 407
Applying a color palette when configuring charts in the View Designer.	“Adding a chart diagram” on page 416
Organizing relationship fields in tab groups in the View Designer.	“Organizing relationship fields in tab groups” on page 433

Table 13. Task Focused UI enhancements (continued)

For information about...	See topic...
Improved usability for disassociating objects. Added a Remove button to grid relationship fields that have an Associate action.	“Adding an Associate action” on page 434
The new Field Groups section in the  > Solution Configuration > Objects task is used to work with field groups.	“Adding field groups to object types” on page 207
The new Field Dependencies section in the  > Solution Configuration > Objects task is used to work with field dependencies.	“Adding and working with dependent fields (Task Focused UI)” on page 279
The new Dependent Picklists section in the  > Solution Configuration > Objects task is used to work with dependent picklists.	“Adding and working with dependent picklists (Task Focused UI)” on page 289
The environment migration tools are now available. Click  > System Migration > Export Configuration and  > System Migration > Import Configuration .	“Exporting configuration items from the source environment (Task Focused UI)” on page 873 “Importing a migration file (Task Focused UI)” on page 877

GRC Workflow

Table 14. GRC Workflow enhancements

For information about...	See topic...
Email reminders can now be configured on standard stages in GRC Workflow.	“Defining a standard stage” on page 519
Users can now complete their workflow tasks in bulk. - Added Bulk Workflow Action to standard stages. - Added functionality to Grid Views to support bulk workflow actions. - Added Complete tasks with bulk workflow actions window to My Tasks tab and panel, Subscription Tasks tab and panel, and Oversight Tasks tab and panel.	“Defining a standard stage” on page 519 “Defining Grid Views for bulk workflow actions” on page 390 “How users interact with workflows ” on page 499
Added Override workflow action text to workflow actions. Use it to customize the text on the confirmation window that is displayed when users select a workflow action.	“Confirm the selected action” on page 501 “Defining a workflow action” on page 527

New and changed features in version 8.2.0.1

New and changed features in version 8.2.0.1 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

IBM OpenPages for IBM Cloud Pak for Data

OpenPages can now be installed on IBM OpenPages for IBM Cloud Pak for Data. For more information, see [Chapter 2, “Administering IBM OpenPages for IBM Cloud Pak for Data,” on page 33](#).

Platform enhancements

Table 15. Platform enhancements	
For information about...	See topic...
New application permissions for the following features: • Watson Language Translator • NPS® Settings • Reg-Track Connector	“Types of application permissions” on page 91
The new Applications > Common > Administration > System Files > Show GRC Folder Structure setting controls whether files for self-contained object types display under system files.	“Configure self-contained object types” on page 636
The new Applications > GRCM > Filtered List > Bulk Update Disabled in Task Focused UI settings controls whether the Bulk Update link displays in Grid Views in the Task Focused UI.	“Disable Bulk Update link in the Task Focused UI” on page 630

Solution enhancements

See the *IBM OpenPages with Watson Solutions Guide* for a complete list of all the changes to solutions.

Table 16. Solution enhancements	
For information about...	See topic...
IBM OpenPages Regulatory Compliance Management includes a new connector to import data from Reg-Track	“Reg-Track Connector” on page 1049

Administration and serviceability enhancements

Table 17. Administration and serviceability enhancements	
For information about...	See topic...
The following new parameter for the LogCollector tool: --location	“Collect log files and diagnostic data” on page 826
Installing tools and utilities, such as ObjectManager, on remote systems	“Installing tools and utilities (IBM OpenPages with Watson)” on page 824

Task Focused UI

Table 18. Task Focused UI enhancements	
For information about...	See topic...
The new Watson Integrations > Watson Language Translator task on the Administration menu is used to integrate a Watson Language Translator service with OpenPages.	“IBM Watson Language Translator” on page 1018
A Net Promoter Score (NPS) survey can now be displayed and submitted directly from OpenPages.	“Configuring a Net Promoter Score (NPS) survey” on page 450
Microsoft Office files can now be opened and edited directly from OpenPages.	“Allow opening Microsoft Office files directly from OpenPages” on page 617
The new  Solution Configuration > Objects task on the Administration menu is used to work with object types and supporting information.	“Working with object types (Task Focused UI)” on page 253
The definition of fields and field groups is included in the  Solution Configuration > Objects task.	Chapter 9, “Fields and field groups,” on page 199 “Defining field groups” on page 206 “Defining fields and adding them to field groups” on page 207
The definition of public filters is included in the  Solution Configuration > Objects task.	“Adding filters to object types (Task Focused UI)” on page 271
Two new data types, Business Entity Selector and User Group, are available on fields. The Display Type attribute is now defined on fields in the Task Focused UI. It is still defined on profiles in the Standard UI.	“Data types” on page 203 Chapter 9, “Fields and field groups,” on page 199 “Defining fields and adding them to field groups” on page 207
The new  Solution Configuration > Profiles task on the Administration menu is used to define profiles.	“Creating a profile (Task Focused UI)” on page 298
The new  Users and Security > Domains & Groups task on the Administration menu is used to define domains and groups.	“Creating an organizational group (Task Focused UI)” on page 88 “Assigning and removing a role from a user or group (Task Focused UI)” on page 117
The new  Users and Security > Role Templates task on the Administration menu is used to provision and modify role templates.	“Adding a role template (Task Focused UI)” on page 114
The new  Users and Security > Security Rules task on the Administration menu is used to define security rules.	“Security rules” on page 120
Safe mode can now be applied to Dashboards.	“Defining a dashboard for a profile” on page 368

GRC Workflow

Table 19. GRC Workflow enhancements	
For information about...	See topic...
Added Ancestor and Descendent as valid values in Relationship Type when choosing a field on a related object in the following places: • Assign To and Adjust Date By on the Overall Due Date field on workflow properties. • Assign To and Due Date on the Due Date field on standard stages. • Add Assignee and Add Subscriber fields on standard stages. • Add User in End Stage Notifications fields on end stages.	“Defining workflow properties ” on page 514 “Defining a standard stage” on page 519 “Defining an end stage” on page 523

New and changed features in version 8.2

New and changed features in version 8.2 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

Platform enhancements

Table 20. Platform enhancements	
For information about...	See topic...
The GRC Calculations feature.	Chapter 14, “Configuring GRC Calculations,” on page 457
The Scheduler feature.	Chapter 16, “Scheduler,” on page 551
The ability to run a GRC Workflow on a schedule.	“Defining workflow properties ” on page 514
The redesigned login page and how you can add a link to an acceptable use policy.	“Defining messages and behavior on the login screens” on page 571
The ability to add a privacy menu item and an acceptable use policy menu item to the Help menu.	“Defining the Privacy and Acceptable Use menu items” on page 574
The new configuration file, <code>openpages-tools-client.properties</code> .	“Tools properties and parameters ” on page 1085
New application permissions for the following features: • GRC Calculations • Scheduler • IBM Watson Assistant (separate application permissions for administrators and users) • Notification Manager • ObjectManager • Administration menu items in the Task Focused UI	“Types of application permissions” on page 91

Table 20. Platform enhancements (continued)	
For information about...	See topic...
The Audit Trail (Change History) application permission also applies to the new Activity tab in Task Views.	“Types of application permissions” on page 91 “Using a Task View” on page 381
Functionality that supported the integration of IBM OpenPages with Watson with IBM Business Process Manager was removed.	
Visualizations that rendered business processes in a graphical format are no longer supported.	
By default, you can now create QuestionnaireAssessments with the Add New wizard. The default value of Applications > GRCM > Add New Wizard > Object Types Disabled has changed. It no longer includes QuestionnaireAssessments.	“Controlling the availability of object types in the Add New wizard” on page 286

Solution enhancements

See the *IBM OpenPages with Watson Solutions Guide* for a complete list of all the changes to solutions.

Table 21. Solution enhancements	
For information about...	See topic...
The new setting for Wolters Kluwer data feeds: Solutions > RCM > WK > Max Days To Get	“Data import settings for Wolters Kluwer feeds” on page 1056
The new connector that enables you to import obligations from Ascent Reg Tech feeds	“Ascent Connector” on page 1039

Administration and serviceability enhancements

Table 22. Administration and serviceability enhancements	
For information about...	See topic...
Properties that are no longer used were removed from the <code>aurora.properties</code> file.	“Aurora properties and parameters” on page 1081
Properties that are no longer used were removed from the <code><server_name>Server<#>-server.properties</code> file.	“OpenPages server properties and parameters” on page 1083
Properties that are no longer used were removed from the <code><server_name>Server<#>-sosa.properties</code> file.	“Sosa properties and parameters ” on page 1084
Properties that are no longer used were removed from the <code>objectmanager.properties</code> file.	“Settings in the ObjectManager.properties file ” on page 893

Table 22. Administration and serviceability enhancements (continued)

For information about...	See topic...
ObjectManager has changed. • The ObjectManager.log file is now created in the directory that you specify in the <loader-file-path> parameter. If the parameter is not specified, the log file is created in the current directory. • The -server parameter is ignored because ObjectManager now runs on the server. • New application permissions are used.	“ObjectManager command line parameters” on page 883
The JSON4J_Apache.jar file is deprecated.	
The default protocol that is used by OpenPages for secure connections (SSL/TLS) is now TLSv1.2.	
You can now install and run the following tools and utilities on a remote system: • ObjectManager • Update Password Encryption Algorithm (UPEA) • chng-sys-password.sh .bat • RpsRpf.sh .bat • Notification Manager	“Installing tools and utilities (IBM OpenPages with Watson)” on page 824

Task Focused UI

Table 23. Task Focused UI enhancements

For information about...	See topic...
The Settings menu was renamed to the Administration menu. It is now organized into categories.	
The new Calculations task on the Administration menu is used to manage calculations.	Chapter 14, “Configuring GRC Calculations,” on page 457
The new Scheduler task on the Administration menu is used to manage jobs.	Chapter 16, “Scheduler,” on page 551
The new Solutions task on the Administration menu is used to manage solution schema visualizations.	“Solution schema visualizations ” on page 250
The new  > Users and Security > Users task on the Administration menu is used to provision and modify users.	“Creating user accounts (Task Focused UI)” on page 83
The new  > Users and Security > User LDAP Configuration task on the Administration menu is used to define LDAP for user provisioning.	“Configuring LDAP access for user provisioning (Task Focused UI)” on page 81

Table 23. Task Focused UI enhancements (continued)

For information about...	See topic...
The new  > Users and Security > Custom Security task on the Administration menu is used to define security access for Project Milestones and Project Action Items.	“Custom security for projects” on page 144
The new  > Users and Security > Encryption Keystore task on the Administration menu is used to configure the encryption keystore.	“Setting up the encryption keystore” on page 147
The new  > System Configuration > System Files task on the Administration menu is used to add and manage system files and folders.	Chapter 8, “System file management,” on page 187
The new  > Watson Integrations > Watson Assistant task on the Administration menu is used to integrate an assistant with OpenPages.	“Configuring the integration between an assistant and OpenPages ” on page 1014
Classifier fields are now displayed using an IBM Watson Insights button and panel.	“Natural language processing services ” on page 1021
The new  > Watson Integrations > Natural Language Classifiers task on the Administration menu is used to define a classifier configuration.	“Defining a Classifier Configuration (Task Focused UI)” on page 1028
The reporting framework can be generated using the new Reporting Framework Generation task on the Administration menu.	“Updating the reporting framework (Task Focused UI)” on page 977
Details about reporting framework generation operations can be viewed using the new Reporting Framework Generation task on the Administration menu.	“Viewing reporting framework details (Task Focused UI)” on page 977
Currency exchange rates can be modified and uploaded using the new Currencies task on the Administration menu.	“Editing, enabling, disabling, and uploading currency exchange rates (Task Focused UI)” on page 215
The reporting schema can be modified using the new Reporting Schema task on the Administration menu.	“Creating or recreating the reporting schema (Task Focused UI)” on page 162
Reporting periods can be created, finalized, and deleted using the new Reporting Periods task on the Administration menu.	“Creating and finalizing a reporting period (Task Focused UI)” on page 579
Object resets can be started using the new Object Resets task on the Administration menu.	“Starting the object reset (Task Focused UI)” on page 592
System Admin Mode can be enabled and disabled from the Task Focused UI.	“Enabling and disabling System Admin Mode” on page 71
Light formatting can now be applied to object text.	“Modifying object text (Task Focused UI)” on page 561
New Gantt charts in chart relationship fields in Task Views and on Dashboards.	“Adding a chart diagram” on page 416

<i>Table 23. Task Focused UI enhancements (continued)</i>	
For information about...	See topic...
New method type and aggregation field for sum, average, min, and max on charts in Task Views and Dashboards.	“Adding a chart diagram” on page 416
A delete action can now be added to grid relationship fields in Task Views.	“Adding a Delete action” on page 438
Multiple Grid Views can now be defined for an object type.	“Defining a Grid View” on page 389
Multiple Creation Views can now be defined for an object type.	“Defining a Creation View” on page 391
New rule type can determine what Creation View is displayed. The rule type is based on the parent object type, if it is known at creation time.	“Defining a Creation View” on page 391
A dashboard can now contain a Search panel.	See “Adding a Search panel” on page 370 for more information.
A grid relationship field for File object type can now contain an Associate action.	“Defining Task Views for file object types” on page 395
Creation Views for files can now use a File Uploader element.	“Defining Creation Views for file object types” on page 393

GRC Workflow

<i>Table 24. GRC Workflow enhancements</i>	
For information about...	See topic...
In applicability, conditions, and validations that are based on a related object, added Relationship Type and Relationship Paths . This makes it easier to associate the related object.	“Defining workflow properties ” on page 514 “Defining an end stage” on page 523 “Defining a workflow action” on page 527 “Defining a workflow action that creates objects” on page 532 “Defining a workflow action that runs a custom action ” on page 535 “Defining a workflow action that locks or unlocks objects” on page 537 “Defining a workflow action that sets fields” on page 539 “Defining a workflow action that starts a workflow” on page 542
Whether workflow information card content is automatically updated when object information changes is now controlled by a registry setting, Platform > Calculation > Refresh Workflow Information Automatically .	“How users interact with workflows ” on page 499
The review process for questionnaire assessments can now be driven by GRC Workflow.	“Configuring questionnaire assessments” on page 991

Table 24. GRC Workflow enhancements (continued)	
For information about...	See topic...
Added Execute As System to workflow properties.	“Defining workflow properties ” on page 514
Added Execute As System to create objects actions.	“Defining a workflow action that creates objects” on page 532
Added Execute As System to custom action .	“Defining a workflow action that runs a custom action ” on page 535
Added Execute As System to lock or unlock objects .	“Defining a workflow action that locks or unlocks objects” on page 537
Added Execute As System to set fields .	“Defining a workflow action that sets fields” on page 539
Added Execute As System to start workflow .	“Defining a workflow action that starts a workflow” on page 542

New and changed features in version 8.1.0.1

New and changed features in version 8.1.0.1 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

Platform enhancements

Table 25. Platform enhancements	
For information about...	See topic...
The new Manage Pages and Templates task on the Settings menu in the Task Focused UI is used to manage reporting folders and define report pages and page templates. In previous versions, reporting folders, report pages, and page templates were accessed in OPX.	“Accessing report pages and page templates (Task Focused UI)” on page 173
OPX has been removed.	

Solution enhancements

See the *IBM OpenPages with Watson Solutions Guide* for a complete list of all the changes to solutions.

Table 26. Solution enhancements	
For information about...	See topic...
Configuring the new Wolters Kluwer connector in IBM OpenPages Regulatory Compliance Management.	“Wolters Kluwer Connector” on page 1054
The new application permission SOX > Administration > WK Feed .	“Types of application permissions” on page 91 and “Wolters Kluwer Connector” on page 1054

Task Focused UI

Table 27. Task Focused UI enhancements	
For information about...	See topic...
Opening a Quick View from a grid relationship field or a tree diagram in a Task View.	“Adding a grid layout” on page 425
Configuring the Add New action for grid and card relationship fields to open a Creation View in a Quick View sidebar or a new tab. In previous versions, the Creation View always opened in a new tab.	“Adding an Add New action” on page 435
Using bulk update in Grid Views to edit field values across multiple objects. Registry settings that determine access to bulk update in the Standard UI are also used in the Task Focused UI.	<i>IBM OpenPages with Watson User Guide</i> “Hide the Bulk Update feature in filtered list views for user profiles” on page 631 “Exclude object types in Filtered List Views from bulk updates” on page 631
Using Why can't I save? to find out why Save is not enabled for an open object in a Task View or Creation View.	“Displaying debug information” on page 397
The overall look and feel of the Task Focused UI changed due to an upgrade in the underlying infrastructure. Some icons changed and some buttons are larger than in previous releases.	

GRC Workflow

Table 28. GRC Workflow enhancements	
For information about...	See topic...
Advanced logic is available in workflow applicability, workflow actions, and workflow end stages.	“Defining workflow properties ” on page 514 “Defining a workflow action” on page 527 “Defining an end stage” on page 523 “Defining a workflow action that creates objects” on page 532 “Defining a workflow action that runs a custom action ” on page 535 “Defining a workflow action that locks or unlocks objects” on page 537 “Defining a workflow action that sets fields” on page 539 “Defining a workflow action that starts a workflow” on page 542
New operators were introduced for hierarchy fields. The operators are In (hierarchy) and Not In (hierarchy). The Equals and Not Equals operators can also be used in hierarchy fields.	

New and changed features in version 8.1.0

New and changed features in version 8.1.0 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

Platform enhancements

Table 29. Platform enhancements	
For information about...	See topic...
The new setting Administration > Settings > Applications > GRCM > Filtered List > Export Disabled Object Types	“Exclude object types in Filtered List Views from export” on page 630
The new setting Administration > Settings > Applications > GRCM > Filtered List > Export Disabled Profiles	“Hide the Export feature in filtered list views for user profiles” on page 630
The new setting Administration > Settings > Applications > GRCM > Filtered List > Bulk Update Disabled Object Types	“Exclude object types in Filtered List Views from bulk updates” on page 631
The new setting Administration > Settings > Applications > GRCM > Filtered List > Bulk Update Disabled Profiles	“Hide the Bulk Update feature in filtered list views for user profiles” on page 631
The Administration > Settings > Applications > GRCM > Filtered List > Number of Levels to Export setting now also applies to exports in the Task Focused UI, where up to five levels can be exported.	“Number of levels to export in the Filtered List View” on page 632
Version numbers were removed from names of profiles. For example, a profile that was named OpenPages RCM 7.3.0. Master in previous releases is now named OpenPages RCM Master. Go to Administration > Profiles to view profiles.	
The new application permission SOX > Administration > Rules Engine	“Types of application permissions” on page 91 and “Processing regulatory events by using rules” on page 1060
The new application permission SOX > Administration > TRRI Feed	“Types of application permissions” on page 91 and “Configuring the Thomson Reuters import” on page 1044
The new setting Administration > Settings > Common > Administration > Currencies > Upload > Maximum Import Rows	“Maximum rows in exchange rate upload file” on page 635

Solution enhancements

See the *IBM OpenPages with Watson Solutions Guide* for a complete list of all the changes to solutions.

<i>Table 30. Solution enhancements</i>	
For information about...	See topic...
Configuring the new Thomson Reuters connector in IBM OpenPages Regulatory Compliance Management.	“Thomson Reuters Connector” on page 1041

Administration and serviceability enhancements

<i>Table 31. Administration and serviceability enhancements</i>	
For information about...	See topic...
The new app-nodb parameter for the OPBackup command. The new parameter backs up everything except the OpenPages database.	“Running the OPBackup command” on page 719
The new app-nodb parameter for the OPRestore command. The new parameter restores everything except the OpenPages database.	“Running the OPRestore command” on page 686

Task Focused UI

<i>Table 32. Task Focused UI</i>	
For information about...	See topic...
The new home page, profile-driven dashboards, and user-configured dashboard panels.	“Home page, dashboard, and tabs in the Task Focused UI” on page 367
The new permission on role templates that enables administrators to configure dashboards by profile: • SOX > Administration > Dashboards	“Setting up the Task Focused UI” on page 363
The new Analytics link in the banner that enables access to the IBM Cognos Analytics.	“Types of application permissions” on page 91
Enhanced formatting for inline guidance.	“Adding inline guidance” on page 400
Relationship fields as key fields in User Guidance.	“Adding user guidance” on page 402
Single stacked bar charts in chart relationship fields in task views.	“Adding a chart diagram” on page 416
Zone-based and count-based heat maps in chart relationship fields in task views.	“Adding a chart diagram” on page 416
Hidden or visible rules can be applied to inline guidance for sections.	“Adding inline guidance” on page 400
When adding files (attachments), multiple versions of the same file can now be added, viewed, and downloaded. The new Versions component can be added to task views for files (SOXDocument) object types.	“Defining Task Views for file object types” on page 395
Import and export is now supported. Up to five object type levels are supported.	“Number of levels to export in the Filtered List View” on page 632

<i>Table 32. Task Focused UI (continued)</i>	
For information about...	See topic...
Enhancements to key items and the new ability to validate actions by using Select an action to validate in a user guidance panel.	“Adding user guidance” on page 402
The new Sibling relationship type on relationship fields.	“Adding and configuring relationship fields on views” on page 413
Application text, object text, and settings can now be defined in the Task Focused UI. Search functionality is greatly enhanced compared to the Standard UI.	“Modifying application text (Task Focused UI)” on page 566 “Modifying object text (Task Focused UI)” on page 561 “Managing settings (Task Focused UI)” on page 597
FastMap import and export can now be used in the Task Focused UI.	“Accessing FastMap to import data and view status (Task Focused UI)” on page 918 “Viewing FastMap import status” on page 925
Business entity selector fields are now supported in Grid Views, Creation Views, and Task Views.	“Adding a business entity selector field ” on page 412
The Configuration Audit Report now tracks changes that are made to dashboards in the Task Focused UI.	“The Configuration Audit Report” on page 771
Dashboards can be migrated from one environment to another environment by using Export Configuration and Import Configuration or the ObjectManager tool.	“Exporting and importing dashboards ” on page 452
If single sign-on (SSO) is used, system notices display on the dashboard.	“Defining messages and behavior on the login screens” on page 571

GRC Workflow

<i>Table 33. GRC Workflow enhancements</i>	
For information about...	See topic...
Users who define workflows in the GRC Workflow Designer now have access to all objects and fields, regardless of their profile. In previous releases, workflows depended on profiles for access to objects and fields.	
Starting workflow instances in bulk with the Start Workflow option from the Workflow List.	“Starting workflow instances in bulk” on page 546
Customizing the summary email notifications that are sent to administrators who start workflow instances in bulk.	“Customizing email notifications for GRC Workflow ” on page 548
Relationship fields as field overrides in workflow properties.	“Defining a standard stage” on page 519

Table 33. GRC Workflow enhancements (continued)

For information about...	See topic...
Adding comments to workflow actions.	“Designing a workflow” on page 505 “Defining a workflow action” on page 527
The new system workflow fields for workflow comments: • System Workflow Fields:Action Comment • System Workflow Fields:Action Comment Date • System Workflow Fields:Action Comment Owner (users or user groups) The new system workflow fields that track the user who completed the last action and the user who started a workflow: • System Workflow Fields:Last Action User • System Workflow Fields:Workflow Start User Oversight users, assignees, and subscribers can be set to these fields. The fields are available in conditions where you can select A field in the current object or A field in a related object.	“System workflow fields” on page 502
Added a variable [\$WORKFLOW_ACTION_USER\$]. It contains the user who completed the current action. It is used in the email template to show the user who sent an email notification.	“Using variables, functions, and fields ” on page 503
Added new variables that can be used in automated workflows to pass values from a rule to the workflow: • [\$RULE_ASSIGNEES\$] • [\$RULE_CRITICALITY\$]	“Using variables, functions, and fields ” on page 503
Validations and operations in a workflow action are now combined in one section, Validations and Operations . You can control the order that they are performed in.	“Defining a workflow action” on page 527
Sections in a task view can be hidden, initially collapsed, or initially expanded per workflow stage.	“Defining a standard stage” on page 519
The new ability by workflow stage to define access control as read-only for non-participants.	“Defining a standard stage” on page 519
Sending email notifications when a workflow ends.	“Defining an end stage” on page 523
Starting another workflow when a workflow ends.	“Defining an end stage” on page 523
The new operation types in workflow actions: • Create objects • Lock or unlock objects • Start a workflow	“Defining a workflow action that creates objects” on page 532 “Defining a workflow action that locks or unlocks objects” on page 537 “Defining a workflow action that starts a workflow” on page 542

Table 33. GRC Workflow enhancements (continued)

For information about...	See topic...
The new Target Objects field on a set fields operation type on a workflow action can be used to set fields on related objects.	“Defining a workflow action that sets fields” on page 539
The new matches any operator on comparison statements in applicability, validations, and conditions. It is available only for enumerated fields.	
The End User option was added to comparison statements in applicability, validations, and conditions. It is available only for enumerated fields.	“Defining workflow properties ” on page 514 “Defining an end stage” on page 523 “Defining a workflow action” on page 527 “Defining a workflow action that creates objects” on page 532 “Defining a workflow action that runs a custom action ” on page 535 “Defining a workflow action that locks or unlocks objects” on page 537 “Defining a workflow action that sets fields” on page 539 “Defining a workflow action that starts a workflow” on page 542
The ability to add oversight users to workflows and assignees and subscribers to stages from multiple sources, for example, a specific user, a field on the current object, and a field on a related object.	“Defining workflow properties ” on page 514 “Defining a standard stage” on page 519
The ability in workflows to reference system workflow fields on related objects. In applicability, conditions, validations, user assignments, and Filter By criteria where you can choose a field in a related object, you can now choose system workflow fields.	“System workflow fields” on page 502
For workflows that are defined to auto-start, a workflow is now launched when an object is created by copying another object. Previously, copy was not supported for auto-start workflows.	“Defining workflow properties ” on page 514
The new Automated option on workflow properties. Automated workflows are used by IBM OpenPages Regulatory Compliance Management.	“Defining workflow properties ” on page 514
The trim function.	“Using variables, functions, and fields ” on page 503

New and changed features in version 8.0.0.3

New and changed features in version 8.0.0.3 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

Platform enhancements

Table 34. Platform enhancements	
For information about...	See topic...
The change to the authentication method for IBM Cloud®. Natural language classifiers now use an API key instead of a user name and password.	If you use natural language classifiers, update them to use an API key. See “Natural language processing services” on page 1021.

Administration and serviceability enhancements

Table 35. Administration and serviceability enhancements	
For information about...	See topic...
The new setting Administration > Settings > Platform > API > Error Responses .	<i>IBM OpenPages with Watson GRC REST API Guide</i>

Task Focused UI

Table 36. Task Focused UI	
For information about...	See topic...
The new graphical interface that you can use to design and preview views.	“Using the View Designer” on page 385
View type and state are now displayed in the header of a view definition.	“Using the View Designer” on page 385
The header of a Task View can now contain integer, decimal, and currency fields. These field types were not supported in previous versions.	“Defining a Task View header” on page 404

New and changed features in version 8.0.0.2

New and changed features in version 8.0.0.2 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

Platform enhancements

Table 37. Platform enhancements	
For information about...	See topic...
The ability to allow character combinations in URLs	“Configure allowed character combinations for URLs” on page 647
The ability to add messages to the log in screen for the Standard UI, the Task Focused UI, and the OPX administrative interface.	“Defining messages and behavior on the login screens” on page 571
The redesigned login screen for the Standard UI, the Task Focused UI, and the OPX administrative interface.	

Table 37. Platform enhancements (continued)	
For information about...	See topic...
Changes to the display of the Reporting Period drop down list. The drop down list is displayed only if you have created at least one reporting period. This change removes a potential distraction for users, and makes more room for other elements in the page header.	
The ability to configure a user to authenticate either against the password stored in OpenPages or against the password in an LDAP server. In addition, you can use multiple LDAP servers to authenticate users, in which case you can specify which LDAP server to use for each user.	“Creating user accounts (Standard UI)” on page 84

Administration and serviceability enhancements

Table 38. Administration and serviceability enhancements	
For information about...	See topic...
The new setting Administration > Settings > Platform > API > Enable Custom REST Service .	“Enable custom REST service” on page 638
Support for the new BYN, MRU, STN, UYW, and VES currency codes. Restriction: You cannot use these codes as the base currency for a deployment.	The BYN, MRU, STN, UYW, and VES codes are now available. For information about how to enable a currency and upload exchange rates, see “Modifying currency exchange rates” on page 213. The MRO code is renamed Old Ouguiya. The STD code is renamed Old Dobra.

Task Focused UI

Table 39. Task Focused UI	
For information about...	See topic...
The ability to use the Task Focused UI on tablets and mobile devices that use the Chrome browser or the Internet Explorer browser, version 11.	
The new GRC Workflow feature.	Chapter 15, “Configuring GRC Workflow,” on page 495
Setting the following new permission on role templates: • SOX > Administration > Workflow	“Setting up GRC Workflow” on page 495

Table 39. Task Focused UI (continued)	
For information about...	See topic...
The <code>associatePrimary actionType</code> in Task Views and Creation Views. The <code>primaryParent</code> property on the <code>associate actionType</code> has been deprecated. Use the <code>associatePrimary actionType</code> instead.	“Adding actions to relationship fields” on page 434
The new <code>severity</code> property that you can use to add warnings to validation rules.	“Controlling error severity on rules” on page 445
The new <code>filterRules</code> property that you can use to add dynamic filters on related objects in Task Views.	“Defining dynamic filters on actions in relationship fields” on page 438
The new <code>defaultFilterRules</code> property that you can use to add filters to Grid Views.	“Defining default filters on Grid Views” on page 406
The ability to apply rules on relationship fields in Creation Views.	“Designing a Creation View” on page 377
The new Display debug info feature.	“Defining a Task View” on page 394
The new ability in the Task Focused UI to use classifier fields to make object associations suggestions using IBM Watson cognitive technology	“Adding a classifier field that makes object association suggestions” on page 430

New and changed features in version 8.0.0.1

New and changed features in version 8.0.0.1 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

Platform enhancements

Table 40. Platform enhancements	
For information about...	See topic...
The ability to exclude fields from the reporting schema	“Excluding fields from a subsystem” on page 293

Administration and serviceability enhancements

Table 41. Administration and serviceability enhancements	
For information about...	See topic...
The new Trigger Configuration Refresh Utility, which refreshes the trigger cache	“Refreshing trigger configurations” on page 198
Additional queries have been added to the log collector output to provide more detailed environment information.	For information about the LogCollector tool, see “Collect log files and diagnostic data” on page 826
Stack traces now include line numbers	

Task Focused UI

Table 42. Task Focused UI	
For information about...	See topic...
Configuring the new Task Focused UI The user interface that has been included with IBM OpenPages with Watson for numerous releases is now called the Standard UI.	Chapter 13, “Configuring the Task Focused UI,” on page 363
Setting the following new permissions on role templates: • SOX > Administration > Task Focused UI • SOX > Administration > User Interfaces > Login to Task Focused UI • SOX > Administration > User Interfaces > Standard	“Setting up the Task Focused UI” on page 363

New and changed features in version 7.4.0

The new and changed features in IBM OpenPages with Watson version 7.4.0 are described in the following sections. For more information, see [IBM OpenPages GRC New Features Guide](#).

Platform enhancements

New and changed features in version 7.4.0 related to IBM OpenPages platform are described in the following tables.

IBM Cognos Analytics V11.1 enhancements

Table 43. IBM Cognos Analytics V11.1 enhancements	
For information about...	See topic...
Adding Cognos Analytics dashboard and story pages to OpenPages by using the new Cognos Analytics Dashboard Redirect page template.	
The predefined reports that are supplied with OpenPages that have been updated to work with IBM Cognos Analytics V11.1.	Chapter 7, “Managing reports,” on page 167
The new application permission: All/SOX/CommandCenter Studios/Cognos Analytics	“Reporting framework permissions” on page 975

Additionally, the **Reporting** menu now contains **Reporting > Cognos Analytics**. The following menu items were removed:

- **Cognos Analysis Studio**
- **Cognos Connection**
- **Cognos Query Studio**
- **Cognos Report Studio**
- **Cognos Workspace**
- **Cognos Workspace Advanced**

Reporting framework enhancements

Table 44. Reporting framework enhancements	
For information about...	See topic...
Configuring multiple framework models and by using the new standard and basic framework models.	“Framework models” on page 951
The new All Models and Selected Models options on Administration > Reporting Framework > Generation .	“Choosing update options in the reporting framework” on page 976
The new templates, Template_Model and TEMPLATE_NAMESPACE, that you can use to quickly create new framework models and namespaces.	“Creating a framework model and namespace using a template ” on page 961
The new Package Name field on computed fields.	“Defining a computed field” on page 227
The new settings in the Administration > Settings > Platform > Reporting Framework V6 folder:	
Configuration > Concurrent Models	“Configuring the number of models that can be concurrently generated” on page 957
Configuration > Sort Order Locale	“Defining the sort order locale ” on page 959
Models > [model name] > Format	“Defining the format for a framework model” on page 962
Models > [model name] > Is Enabled	“Enabling a framework model ” on page 962
Models > [model name] > Mode	“Defining the query mode for a framework model ” on page 962
Models > [model name] > Profile	“Defining whether a framework model uses profile filtering” on page 963
Models > [model name] > Namespaces > [namespace name] > Is Facts and Dimensions Enabled	“Defining whether facts and dimensions are enabled for a namespace ” on page 965
The Administration > Settings > Platform > Reporting Framework V6 > Models setting has been changed.	“Defining a name for a framework model” on page 961

Administration and serviceability enhancements

New and changed features in version 7.4.0 related to IBM OpenPages administration and serviceability are described in the following tables.

Administration and serviceability enhancements

Table 45. Administration and serviceability enhancements	
For information about...	See topic...
The new New Folder Name field that you can use to give a folder a name when you select a folder under the Administration > Settings menu and click Copy to .	“Copying settings and folders ” on page 634

<i>Table 45. Administration and serviceability enhancements (continued)</i>	
For information about...	See topic...
The new Administration > Manage System Files menu item that allows you to manage system files and folders.	Chapter 8, “System file management,” on page 187
The new ready-to-use OpenPages Platform 3 profile that administrators need to access system files and folders using Administration > Manage System Files .	Chapter 8, “System file management,” on page 187 “Associating users and groups to a profile” on page 302
The new Administration > Settings > Applications > Common > Disable the files of OPX setting that can temporarily enable the OPX interface.	
The new Administration > Settings > Applications > GRCM > Environment Migration > Allow ObjectManager XML setting that controls whether ObjectManager XML files can be imported through Administration > Import Configuration .	“Settings that apply to environment migration” on page 865
The Administration > Settings > Applications > Common > Configuration > Force Internet Explorer Compatibility Mode registry setting has been removed. Internet Explorer 11 in Native mode is supported. Internet Explorer 9 and 10 and Internet Explorer in Compatibility View mode are no longer supported.	
You no longer need to modify the <code>framework.properties</code> file and regenerate the reporting framework when you change the password of the user account that is used by Cognos for updating the reporting framework.	

User provisioning enhancements

<i>Table 46. User provisioning enhancements</i>	
For information about...	See topic...
The new Users menu item on the Administration menu.	Chapter 4, “Users, groups, and domains,” on page 73
Tasks that you should complete before creating, modifying, or copying users and changes to the way delegated administration works in 7.4.0.	“Planning user administration” on page 73
Administrative permissions that are required for each of the user provisioning tasks.	“Administrator permissions for user-provisioning functions” on page 77
LDAP server integration for creating new user accounts.	“LDAP and user provisioning” on page 81
The new method of adding new user accounts with the Create User wizard.	“Creating user accounts (Standard UI)” on page 84
The new method of modifying and managing existing user accounts.	“Modifying user accounts” on page 86

Table 46. User provisioning enhancements (continued)

For information about...	See topic...
The new functionality that allows you to copy a user's locale, profiles, group memberships, and direct role assignments.	“Copying access from one user to another” on page 87
The new registry settings for configuring the behavior of user provisioning functionality.	“User provisioning settings” on page 603
The new default password expiry behavior that uses the Applications > Common > Administration > User Provisioning > Default User Password Expiration setting rather than the OpenPages > Platform > Security > Password > Policy > Default Expiry Days setting.	“Default User Password Expiration” on page 605
When you configure user and group selector display types for simple strings, you can now leave the Starting Group value blank. A blank value used in combination with an Include Disabled value of true can result in improved search performance.	Table 139 on page 354

New features in version 7.3.0.3

The new features in IBM OpenPages with Watson, version 7.3.0.3, are described in the following sections.

Specify the browsers that can access OpenPages

A new registry setting has been added: **Administration > Settings > Applications > Common > Configuration > Allowed Browsers**

Use this setting to create a list of browsers or browser versions that can access OpenPages. For more information, see [“Specify the browsers that can access IBM OpenPages” on page 603](#).

New features in version 7.3.0.2

The new features in IBM OpenPages with Watson, version 7.3.0.2, are described in the following sections.

Cognitive services

Administrators can configure the cognitive services to support decision making when users associate objects.

- Added **Type** and **Field Association** fields to **Administration > Cognitive Services > Natural Language Classifiers**. For more information, see [“Natural language processing services ” on page 1021](#).

Integration with IBM Regulatory Compliance Analytics

Administrators can configure how IBM Regulatory Compliance Analytics data is imported into IBM OpenPages with Watson.

Added **RCA Integration** to the **Administration** menu. It has two menu items:

- **Configure Import from RCA**
- **Import from RCA**

Added the application permission, RCA Integration, which controls whether these menu items are displayed. It is located in **SOX > Administration**. Administrators who work with IBM Regulatory

Compliance Analytics integration need to have this application permission. For more information, see [“Types of application permissions”](#) on page 91.

Registry settings for third-party SMTP providers

Added registry settings:

- **Applications > Common > Email > SMTP Port**
- **Applications > Common > Email > SMTP Security Type**

Define these settings if you use a third-party SMTP provider. For more information, see [“Set the mail server address”](#) on page 612.

Auto-naming setting for SOXDocument objects

You can use the new Auto Remediate Duplicate File Names setting to control auto-naming for SOXDocument objects if file names are not unique in a folder. For more information, see [“SOXDocument object auto-naming settings for duplicate file names”](#) on page 611.

Copy views to profiles

Administrators can now copy object and creation views from one profile to one or more other profiles. For more information, see [“Copying views for an object from one profile to one or more other profiles”](#) on page 330.

Configuring user-friendly URL link names by using the rich text display type for simple strings

You can use the rich text display type to display a user-friendly link name as a field's default value. For example, you can configure a field's default value to display as **My Company** rather than **http://www.mycompany.com**. This existing feature is described in the new topic, [“Configuring URL link names by using the rich text display type for simple strings \(Standard UI\)”](#) on page 352.

Compare environments

You can find differences between two environment configuration XML files by using **Compare Environments**. Use Compare Environments to identify and resolve issues before you migrate configurations from one environment to another. For more information, see [Chapter 25, “Comparing IBM OpenPages with Watson environments,”](#) on page 853.

New features in version 7.3.0.1

The new features in IBM OpenPages with Watson, version 7.3.0.1, are described in the following sections.

Cognitive services

- Added the data type, Classifier. A classifier field must have this data type.
For more information, see [“Data types”](#) on page 203.
- Added the menu item, **Administration > Cognitive Services > Natural Language Classifiers**. Use this task to create a classifier configuration. For more information, see [“Natural language processing services”](#) on page 1021.

UCF connector integration

Use IBM OpenPages SDI Connector for UCF Common Controls Hub to import data from UCF Common Controls Hub into IBM OpenPages with Watson.

For more information, see [“IBM OpenPages SDI Connector for UCF Common Controls Hub integration” on page 986.](#)

IBM OpenPages Regulatory Compliance Management Theme Deployer

The RCM Theme Deployer is a tool that users can use to lay the foundation for business entities to complete regulatory compliance assessments.

For more information, see [“RCM Theme Deployer” on page 1065.](#)

IBM OpenPages Regulatory Compliance Management configuration tool

You can use the IBM OpenPages Regulatory Compliance Management tool to configure the RCM solution, including the RCM Theme Deployer.

For more information, see [Chapter 37, “Configuring IBM OpenPages Regulatory Compliance Management,” on page 1039.](#)

New X-XSS-Protection response header setting

The new **X-XSS-Protection** setting enables XSS filtering on server responses. Using this setting is preferred to using the **IE XSS Filter** setting. If there is a conflict between the **IE XSS Filter** and **X-XSS-Protection** settings, the one that enables the header is used. For more information about **X-XSS Protection**, see [“Configure the HTTP response headers” on page 647.](#)

New features in version 7.3.0

The new features in IBM OpenPages with Watson Version 7.3.0 are described in the following sections.

Enable or disable file attachment search

From the global search administration page, you can now toggle between enabling and disabling the file attachment search component for all search-enabled file types.

For more information, see [“Enabling and disabling file attachment searching” on page 654.](#)

Specify which file types are enabled for file attachment search

From the SOXDocument object type administration page, you can specify which MIME (Multipurpose Internet Mail Extensions) types are enabled or disabled for file attachment global search.

In a new installation of OpenPages 7.3, some MIME types are enabled for searching and others not. When you upgrade to OpenPages Version 7.3.0 from an earlier version, the same set of MIME types are enabled. However, the Search Files switch is off so that existing customers can continue to use global search with the existing functionality.

For more information, see [“Enabling attachment file types for global search” on page 654.](#)

Show an additional custom field in the search results

You can now configure one additional custom field to be displayed in the search results for each object type. As administrator, you can customize global search results to contain one additional field in the search results to help the user determine whether the record that is returned is the record for which they want the details.

For more information, see [“Displaying a custom field in global search results” on page 659.](#)

Legacy option for the new copy and associate functionality

You can use a registry setting to revert to using the legacy copy and associate features in Activity Views and Detail Views only. This is to allow time to ensure that the new implementation meets your needs

before you retire the old implementation. The interface that is used for copy tasks and for associate tasks from Grid Views is always the new interface.

For more information about the legacy copy setting, see [“Set copy operations” on page 614](#).

For more information about the legacy associate setting, see [“Common folder settings” on page 635](#).

Dashboard tab for the user's home page

The Dashboard tab allows users to create their own dashboard for the Home Page. Users can now make their workflows more efficient by creating quick access to the tasks and information that they use most often. Users can tailor their dashboards to suit the way that they work.

Users and administrators can add as many of the following types of widgets as needed to the Dashboard tab:

- Filter Count widget
- Object Global Search widget
- Static Web Link widget
- Add New widget, which creates a **Add New** button that is preconfigured for a specific object type.

For each profile, administrators can create a default Dashboard tab that is displayed for users who log on to OpenPages for the first time. Administrators can specify that a panel is either locked or unlocked. When a locked panel is saved by an administrator, it is automatically pushed to the Dashboard tab of all users in the profile the next time those users log on. When an unlocked panel is saved by an administrator, it becomes part of the default Dashboard tab for users who are opening the application for the first time, but the panel is not pushed to the Dashboard tab of users. Users can edit or delete unlocked panels but cannot edit or removed locked panels.

For more information, see [“Configuring users' Dashboard tabs” on page 319](#).

Integration with IBM Business Process Manager

Added the following registry settings in the **Administration > Settings > Platform > Workflow Implementations > IBM BPM** folder:

- **Enable Login SSO**
- **Portal Page Path**
- **Server URL**

Added the following menu items to the **Administration** menu:

- **IBM BPM Process Center**
- **IBM BPM Process Inspector**
- **IBM BPM Process Admin**

Added the new application permission, IBM BPM, which controls whether these menu items are displayed. It is located in **SOX > Administration**. Administrators who work with IBM BPM need to have this application permission.

To profiles, added **Process Portal** to the Home Page Tab Configuration setting. When this setting is set to **Visible**, the **Process Portal** tab is displayed on the Home Page.

Personalizations are now maintained

Some personalizations to OpenPages are now maintained when you clear your browser cache or switch to another browser or device. For example, if you rearrange the panels on your home page dashboard and then switch to another browser, your dashboard looks the same in the new browser window. The changes that you made to the panels are preserved. Previously, personalizations were lost because they were stored in the browser.

In version 7.3, the following personalizations are stored in the database:

- The home page tab that was last selected: **My Work** or **Dashboard**
- **My Work** tab
 - Hidden and shown panels
 - Collapsed and expanded panels
 - Panel sequence
- **Dashboard** tab
 - Hidden and shown panels
 - Panel sequence
 - Widgets added and removed from the dashboard
- Analytics bar:
 - The default filter
 - The filters that are displayed on the analytics bar
 - The order of the filters
 - The expanded or collapsed state of the analytics bar
- Grid views
 - Column widths
 - Sequence of fields
 - Compact mode or full mode, and the fields shown or hidden for each mode

Enhanced export functionality

Using new registry settings, you can:

- allow users to choose which object types and fields to export. For more information, see [“Enable object type and field export choices in the Filtered List View”](#) on page 629.
- exclude object types from an export unless they are included in the Filtered List View. For more information, see [“Exclude object types from exports if they are not in a Filtered List View”](#) on page 629.
- determine how many total levels of object types the user can choose to export, including the top-level object that is exported. For more information, see [“Number of levels to export in the Filtered List View”](#) on page 632.

FastMap import performance improvements

The performance of FastMap imports has been improved by a significant amount. The improved performance applies to objects being created or updated.

Note: The total time it takes to modify objects with a FastMap import can be affected by the time it takes for the triggers to operate. The improvements made to FastMap import performance do not impact the portion of time spent evaluating and executing the triggers.

Disable Add New capability

You can now disable the **Add New** capability from several launch points within the product by using one or more new registry settings. This is useful if users find it difficult to select the most appropriate parent information for particular object types.

For more information, see [“Disable the Add New wizard from various launch points”](#) on page 600.

Collect and view logs

The new LogCollector tool provides a command-line interface that you can use to collect log files and diagnostic data from the IBM OpenPages with Watson environment.

With the LogCollector tool, you can collect log and diagnostic files from the IBM OpenPages with Watson environment and from the IBM OpenPages with Watson database.

Chapter 2. Administering IBM OpenPages for IBM Cloud Pak for Data

IBM OpenPages for IBM Cloud Pak for Data 8.2 is an integrated governance, risk, and compliance platform that companies can use as a tool to assist in managing risk and regulatory challenges across the enterprise.

It provides a set of core services and functional components that span risk and compliance domains, which include operational risk, policy management, financial controls management, IT governance, internal audit, model risk governance, regulatory compliance management, third-party risk management, and business continuity management.

IBM OpenPages for IBM Cloud Pak for Data provides a powerful, highly scalable, and dynamic tool set that helps empower managers with information transparency and the capability to identify, manage, monitor, and report on risk and compliance initiatives on an enterprise-wide scale.

Documentation for IBM OpenPages for IBM Cloud Pak for Data administrators

Some administrative tasks do not apply in IBM OpenPages for IBM Cloud Pak for Data. Use the following table to help you find the information that's relevant to IBM OpenPages for IBM Cloud Pak for Data.

For information about...	See
Setting up users and groups	“Managing users and groups within IBM Cloud Pak for Data” on page 35
• Connecting to your LDAP server • Configuring SAML single sign-on	Managing users
Security	• “Role-based security model” on page 105 • “Security rules” on page 120
Setting up the object model (object types, profiles, fields, and field groups)	• Chapter 10, “Object types,” on page 249 • Chapter 11, “Profiles,” on page 297 • Chapter 9, “Fields and field groups,” on page 199 • Chapter 6, “Managing the reporting schema ,” on page 159
Configuring the home page and dashboards	“Home page, dashboard, and tabs in the Task Focused UI” on page 367
Creating views	• Chapter 13, “Configuring the Task Focused UI,” on page 363 • “Views in the Task Focused UI” on page 370 • “Using the View Designer” on page 385 • Chapter 31, “Configuring questionnaire assessments ,” on page 991
Creating calculations	Chapter 14, “Configuring GRC Calculations,” on page 457
Designing and creating workflows	Chapter 15, “Configuring GRC Workflow ,” on page 495

For information about...	See
Scheduling jobs	Chapter 16, “Scheduler,” on page 551
Localizing text in the application user interface	Chapter 17, “Localizing text,” on page 559
Importing and exporting data	• Chapter 28, “Using FastMap ,” on page 915: A user interface for importing and exporting data • Chapter 27, “The ObjectManager tool,” on page 881: A command-line tool for importing and exporting data To install ObjectManager, see “Installing tools and utilities (IBM OpenPages with Watson)” on page 824.
Environment configuration and system maintenance	• “Managing settings (Task Focused UI)” on page 597: Some settings do not apply in IBM OpenPages for IBM Cloud Pak for Data environments • Chapter 8, “System file management,” on page 187 • Appendix B, “Properties and parameters,” on page 1081: Describes the properties and parameters in configuration files • “Auditing configuration changes” on page 770 • “Installing tools and utilities (IBM OpenPages with Watson)” on page 824 • “Starting and stopping application servers in IBM OpenPages for IBM Cloud Pak for Data” on page 41 • “Changing the password of the OPSys user in IBM OpenPages for IBM Cloud Pak for Data” on page 57 • “Changing the password of the Liberty keystore in IBM OpenPages for IBM Cloud Pak for Data” on page 58 • “Logging in to the database in IBM OpenPages for IBM Cloud Pak for Data” on page 67
Configuring apps and integrations	• “IBM Watson Assistant ” on page 1013 • “IBM Watson Language Translator” on page 1018: You can integrate with a service instance that is hosted on IBM Cloud • IBM OpenPages SDI Connector for UCF Common Controls Hub: See the <i>IBM OpenPages with Watson Installation and Deployment Guide</i> • “Natural language processing services ” on page 1021: You can integrate with IBM Watson Discovery on IBM Cloud Pak for Data or the Natural Language Classifier service on IBM Cloud • Chapter 34, “Configuring OpenPages Loss Event Entry,” on page 1003 • “Updating IBM OpenPages Model Risk Governance for integration with OpenScale” on page 67
Configuring connectors for data feeds	• “Ascent Connector” on page 1039 • “Reg-Track Connector” on page 1049 • “Thomson Reuters Connector” on page 1041 • “Wolters Kluwer Connector” on page 1054 • “SecurityScorecard connector for IBM OpenPages Third Party Risk Management” on page 1071

For information about...	See
	• “Supply Wisdom connector for IBM OpenPages Third Party Risk Management” on page 1073
Best practices and troubleshooting	• Appendix E, “Best practices for configuring IBM OpenPages with Watson,” on page 1109 • Appendix D, “Troubleshooting and support for IBM OpenPages with Watson,” on page 1097

Managing users and groups within IBM Cloud Pak for Data

In IBM OpenPages for IBM Cloud Pak for Data, a group name `CloudPak_Members` is created for you in OpenPages during provisioning. You create your own users and groups in Cloud Pak for Data, rather than in OpenPages, and those users and groups are created in the `CloudPak_Members` group in OpenPages. The users and groups are created and configured in OpenPages by a synchronization job that runs on a schedule.

You still manage role templates, profiles, and locales in OpenPages.

Adding users

You can add users in Cloud Pak for Data so that you can give them access to an OpenPages instance.

About this task

To add users, you use the default administrator account to log in to Cloud Pak for Data web client and complete the following steps:

Procedure

1. On the Cloud Pak for Data welcome page, click **Manage users**.
2. Click **Add user**.
3. On the **Profile information** page, enter the following information:

- **Username**
- **Email**

If you don't enter an email address, the user will not have an email address in OpenPages either. If you try to enter an email address in OpenPages, the synchronization job will remove it. This is important because some OpenPages features, such as workflow notifications and NPS surveys, require a user's email address.

- **Password**
- **Confirm password**

4. Click **Next**.
5. On the **Platform access** page, select **Assign roles directly**.
6. Click **Next**.
7. On the **Roles** page, select **User**.
8. Click **Next**.
9. On the **Summary** page, click **Add**.

What to do next

Now you need to give the user access to the OpenPages instance. For more information, see [“Managing access to OpenPages instances” on page 36](#).

Managing access to OpenPages instances

A default admin user is created by Cloud Pak for Data to be used to configure access, such as connecting with LDAP, configuring single sign-on, and creating users and groups. Admin users can perform administrative tasks on an OpenPages instance, such as scaling the instance and adding or removing other users.

If you are using an LDAP server for user management, you can further secure your Cloud Pak for Data system by disabling the default admin user. For more information, see [Disabling the default admin user](#).

Note: If you want a user to be an OpenPages super administrator, create the user first in Cloud Pak for Data and, once the synchronization job has run, you can go into the OpenPages instance and set the user's **Super Administrator** property to **True**. For more information, see [“Creating a Super Administrator” on page 75](#).

About this task

To specify which users can access an OpenPages instance, you use the default administrator account to log in to Cloud Pak for Data web client and complete the following steps:

Procedure

1. On the Cloud Pak for Data welcome page, click **Overview > Instances**.
Alternatively, you can click **ServicesInstances** in the navigation menu.
2. From the instances list, click the instance you want to modify.
Tip: OpenPages instances always have a name containing "openpages".
3. Click the options menu and select **Manage access**.
4. To give a user access to the OpenPages instance, perform the following steps:
 - a) Click **Add users**.
 - b) In the **Grant access to users** dialog box, select a user and select the **OpenPagesUser** service role.
 - c) Click **Add**.
5. To remove a user's access to the OpenPages instance, perform the following steps:
 - a) Click the **Remove** icon in the row with the name of the user you want to remove.
 - b) When the **Remove this user?** dialog box is displayed, click **Remove**.

What to do next

Because users will be logging in through Cloud Pak for Data, you will need to provide the users with the URL, user name, and password they need to access it. As an administrator, you can set up a custom route for your users to be able to log in. For more information, see [Creating a custom route to the platform](#).

How users and groups are synchronized from Cloud Pak for Data to OpenPages

In IBM OpenPages for IBM Cloud Pak for Data, you create and configure users and groups in Cloud Pak for Data and then they are synchronized to OpenPages.

- All of the users and groups created in Cloud Pak for Data are created under the CloudPak_Members group in OpenPages. Users are created with the default locale as it was configured for the user and group synchronization job.
- All users are created with default profiles as configured by the synchronization job unless the user has already been assigned to a group associated with other profiles. You can assign profiles to a group in OpenPages using **System Configuration > Settings > Platform > CloudPak > Sync > Profiles** settings.
- Roles of users and groups created in Cloud Pak for Data are not transferred to OpenPages.

OpenPages administrators are able to change locale, profiles, and roles directly from within OpenPages. These settings take precedence over settings in Cloud Pak for Data and will not be overridden when a synchronization job runs.

For example, an OpenPages administrator can assign a profile to a user based upon its group affiliation as a key (profile name) and comma-separated values (group name) in **System Configuration > Settings > Platform > CloudPak > Sync > Profiles** settings folder.

Important: If an OpenPages administrator maps a profile to a group in OpenPages using **System Configuration > Settings > Platform > CloudPak > Sync > Profiles** settings, and the user and group in this mapping have already been synchronized before, the change to the mapping is not detected the next time the synchronization job runs. To make sure that the synchronization job picks up the change, use **Manage access** in Cloud Pak for Data to change the **Full name** field for the user. After the synchronization runs, you can change the **Full name** field for the user back to what it was.

Properties that will be overwritten in OpenPages by the user synchronization job

Because users and groups are synchronized from Cloud Pak for Data, if you change the following properties in OpenPages, your changes will be overwritten when the synchronization job runs.

User properties

- User Name
- First Name
- Last Name
- Email
- Description
- All fields in Password and Security

Group properties

- Description

Adding and changing users and groups

The following table shows what happens when you create and modify users and groups.

Action	Outcome
Create a group in Cloud Pak for Data and assign that group to the OpenPages instance. You can add existing users to the new group.	In OpenPages, if the group has users, it is created with name and description as specified in Cloud Pak for Data. The group is a subgroup under the CloudPak_Members group and existing users added to the group in Cloud Pak for Data are associated with the group in OpenPages.

Action	Outcome
Create a user in Cloud Pak for Data.	In OpenPages, the user is a member of the CloudPak_Members group by default. • User Name, Display Name, Email, and Group association come from Cloud Pak for Data. • The locale is the Default Locale configured in the synchronization job's parameters. • If an OpenPages administrator mapped profiles to an associated group using System Configuration > Settings > Platform > CloudPak > Sync > Profiles settings, the unique list of Available Profiles corresponds to that group association. Otherwise, the Available Profiles is the default as configured in the synchronization job's parameters. • The Preferred Profile is first of the Available Profiles when sorted alphabetically. Otherwise, the Preferred Profile is the default as configured in the synchronization job's parameters. Note that new users are not assigned a Role Template. The OpenPages administrator assigns Role Templates.
Change the name of a group in Cloud Pak for Data.	A new group is created in OpenPages with the new name in the CloudPak_Members group. The group with the old name is moved into the Standalone Users and Groups group. Users are disassociated from the group in Standalone Users and Groups and associated with new group.
Change the description of a group in Cloud Pak for Data.	The description of the group changes in OpenPages.
Change the groups a user is associated with in Cloud Pak for Data.	The group associations in OpenPages change to match that in Cloud Pak for Data.
Delete a group in Cloud Pak for Data.	In OpenPages, the group is moved from the CloudPak_Members group to the Standalone Users and Groups in OpenPages. Users associated with that group that are members of other groups are no longer associated with the deleted group. Users not associated with other groups have their status changed to Inactive .
Delete a user in Cloud Pak for Data.	The status of the corresponding user in OpenPages is set to Inactive .
Remove a user from the list of users that can access the OpenPages instance in Cloud Pak for Data.	The status of the corresponding user in OpenPages is set to Inactive . For more information on removing a user from the list of users that can access the OpenPages instance, see “Managing access to OpenPages instances” on page 36 .
In Cloud Pak for Data, recreate a user that was previously deleted.	The status of the corresponding user in OpenPages is set to Active .

Action	Outcome
Recreate a group in Cloud Pak for Data that was previously deleted.	In OpenPages, the group that was deleted moves from the Standalone Users and Groups group to the CloudPak_Members group. If there are any users in this new group, they are associated with the recreated group.

Configuring the user and group synchronization job

The user and group synchronization job is a Kubernetes cronjob.

About this task

The synchronization job can be configured with the following parameters:

Parameter	Default value	Description
SYNCH_FROM_SERVICE_INSTANCE	true	By default, the synchronization runs for groups and users assigned to the OpenPages service instance in Cloud Pak for Data. If set to false, the synchronization happens directly for groups and users at the Cloud Pak for Data platform level.
DEFAULT_LOCALE_ISO_CODE	en_US	By default, all users are created in OpenPages with locale set to the value of this parameter.
DEFAULT_PREFERRED_PROFILE_NAME	OpenPages Modules Master	Users are created in OpenPages with Current Profile set with the value of this parameter if profiles are not already mapped to groups in OpenPages under System Configuration > Settings > Platform > CloudPak > Sync > Profiles settings.
DEFAULT_AVAILABLE_PROFILE_NAME	OpenPages Modules Master	Users are created in OpenPages with Allowed Profiles set with the value of this variable if profiles are not already mapped to groups in OpenPages under System Configuration > Settings > Platform > CloudPak > Sync > Profiles settings. This parameter contains comma separated values.

Procedure

1. Log in to the OpenShift cli.

You can also use the OpenShift Container Platform Web console. For more information, see "Accessing the web console" in the RedHat OpenShift documentation.

2. Run the following command to edit the cronjob parameters:

```
oc edit cronjob $(oc get cronjobs | grep user-sync-cron-job | awk -F " " '{print $1}')
```

Save the changes.

Checking running synchronization jobs

You can view the last three user synchronization jobs that ran.

About this task

Procedure

1. Log in to the OpenShift cli.

You can also use the OpenShift Container Platform Web console. For more information, see "Accessing the web console" in the RedHat OpenShift documentation.

2. Run the following command:

```
oc get pods | grep user-sync-cron-job
```

Files and directories in IBM OpenPages for IBM Cloud Pak for Data

The locations of files and directories in IBM OpenPages for IBM Cloud Pak for Data is different than in IBM OpenPages with Watson.

Use the following table to help you locate files and directories in IBM OpenPages for IBM Cloud Pak for Data.

Table 47. Files and directory paths for IBM OpenPages for IBM Cloud Pak for Data	
File or directory	Location in IBM OpenPages for IBM Cloud Pak for Data
<OP_HOME>	/opt/ibm/OpenPages/
<WLP_HOME>	/opt/ibm/wlp/
<WLP_USER_HOME>	/opt/ibm/wlp/usr/
<JAVA_HOME>	/opt/ibm/java/jre
<OP_BACKUP_RESTORE>	/opt/ibm/OpenPages/openpages-backup-restore
Application server configuration files • server.properties • sosa.properties • bootstrap.properties	/opt/ibm/wlp/usr/servers/defaultServer/
Application properties: aurora.properties	/opt/ibm/OpenPages/aurora/conf/aurora.properties
Application WAR files	/opt/ibm/wlp/usr/servers/defaultServer/apps/ expanded/op-apps.ear/taskui.war/
Application server configuration overrides directory	/opt/ibm/wlp/usr/servers/defaultServer/ configDropins/overrides
Keystore files	/opt/ibm/wlp/output/defaultServer/resources/ security/
Log files	You can collect and view logs by using the Diagnostics feature in the OpenShift® web client.

Starting and stopping application servers in IBM OpenPages for IBM Cloud Pak for Data

You can use the following methods to start and stop application servers in IBM OpenPages for IBM Cloud Pak for Data.

Table 48. Starting and stopping servers	
To do this...	Do these steps
Restart all application server pods by using the Red Hat® OpenShift UI	1. Log in to the Red Hat OpenShift web client as an administrator. 2. Click Workload > StatefulSets, and then click openpages- <instance_name>-sts. 3. Decrease the number of pods to 0. Wait for all pods to be removed. 4. Increase the number of pods to the value that you use in your environment.
Restart all application server pods by using the Red Hat OpenShift command line	1. Log in to the cluster as an administrator. 2. Go to the project where IBM Cloud Pak for Data is installed. <pre>oc project <Project></pre> 3. Scale down to 0 replicas: <pre>oc scale --replicas=0 sts/openpages-<instance_name>-sts</pre> 4. Wait until all application server pods are deleted. 5. Scale up to the number of replicas you want to use for the application server: <pre>oc scale --replicas=<#_of_replicas> sts/openpages-<instance_name>-sts</pre>
Start the application server within a pod	1. Log in to the pod: <pre>oc exec -it <pod name> -- /bin/bash</pre> 2. If you are using an external database, run the following command: <pre>source /opt/ibm/openpages/bin/provision-dbsecrets.sh</pre> 3. Start the application server: <pre>/opt/ibm/wlp/bin/server start</pre>
Stop an application server within a pod	1. Log in to the pod: <pre>oc exec -it <pod name> -- /bin/bash</pre> 2. Stop the application server: <pre>/opt/ibm/wlp/bin/server stop</pre>

Integrated reporting with Cognos Analytics

You can configure IBM OpenPages for IBM Cloud Pak for Data instances to use Cognos Analytics for your organization's reporting requirements.

Integration overview

You can set up the integration with Cognos Analytics when you provision an OpenPages instance. You can also set up the integration for instances that already exist.

The Cognos Analytics instance and the OpenPages instance must be installed in the same instance of IBM Cloud Pak for Data.

You can integrate multiple OpenPages instances with a single Cognos Analytics instance.

After you set up the integration, you enable Cognos Analytics in your OpenPages instance and generate the reporting framework.

For more information, see [“Adding Cognos Analytics to OpenPages” on page 43](#).

Reporting framework

The reporting framework consists of Cognos Analytics framework models. The models support relational data used for creating reports in Cognos Analytics.

If you've used OpenPages on-premises, you'll notice that the options for framework generation have changed. IBM OpenPages for IBM Cloud Pak for Data uses a different, streamlined process to generate reporting frameworks.

In IBM OpenPages for IBM Cloud Pak for Data

- Custom query subjects are stored in the aurora directory in the app server pod.
- Facts and dimensions are not supported.
- Only Dynamic Query Mode (DQM) framework models are supported.
- Some out-of-the-box reports are not available:
 - Configuration Audit
 - Process Log Report
 - Process Log Report Full Detail
 - Audit Summary
 - Auditor Timesheet Dashboard
 - Auditor Utilization Dashboard
 - Auditor Utilization Dashboard drilldown
 - Auditor Utilization Detail
 - Pending Timesheet Approvals Dashboard
 - Pending Timesheet Approvals Detail
 - Auditor Deviation
 - Process Control Effectiveness by Mandate
 - Risk Assessment Status & Details report
 - Risk Heat Map & Risk Detail report
 - Risk Rating by Category & Detail report
 - Risk Rating by Entity & Detail report

Adding Cognos Analytics to OpenPages

You can configure IBM OpenPages for IBM Cloud Pak for Data instances to use Cognos Analytics for your organization's reporting requirements.

Before you begin

- The Cognos Analytics instance and the OpenPages instance are installed in the same instance of IBM Cloud Pak for Data.
- A Cognos Analytics 4.0.3 or later instance is running.
- An OpenPages 8.204.0 or later instance is running.

Procedure

1. If you did not enable the integration when you provisioned OpenPages, do the following steps:
 - a) Update the OpenPagesInstance CR to set `enableIntegrationWithCognos: true`. You can make this update either through the IBM Cloud Pak for Data web client or by using the command line.

For the command line, run the following command to open the CR for editing:

```
oc edit -n cpd-instance OpenPagesInstance <instance_name>
```

- b) Wait until the status of the process is **Complete**.
2. Log in to OpenPages as an administrator.
 3. Click  > **Integrations** > **Cognos Analytics**.
 4. Optional: In the **OpenPages Instance Name**, type the name that you want to use for the integration in Cognos Analytics. The default value is the name of your OpenPages instance.

For example, if you use `openpagesinstance1`, the folder in Cognos Analytics will be `Team content/openpagesinstance1`.

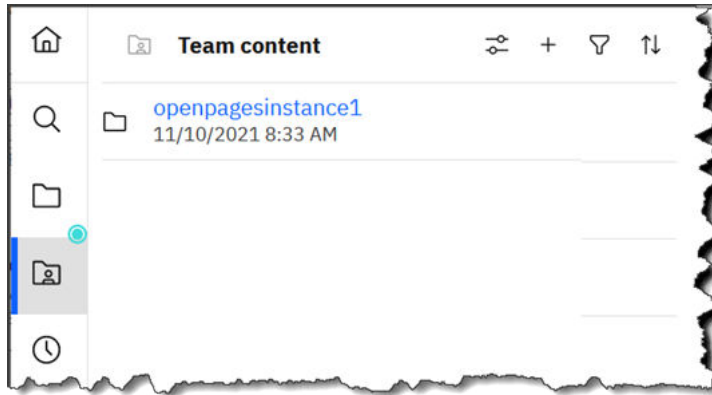


Figure 1. OpenPages integration folder in Cognos Analytics

You can, for example, use a folder that is called `Dev`, and then later use another that is called `UAT`. Your OpenPages instance can use only one folder at a time, but you can switch between them by updating the **OpenPages Instance Name** field.

5. Click **Enable**.
6. Click **Submit**.
7. Refresh OpenPages by doing the following steps:
 - a) Close all OpenPages browser windows.
 - b) Open a new incognito or private window.

Or, clear the OpenPages session cookies, which are called `OPJSESSIONID-POD<N>`.

For example, in Chrome, go to **Settings > Privacy and security**. Click **See all cookies and site data**. Click the OpenPages URL, and then delete the OPJSESSIONID-POD<N> cookies.

8. Update the reporting framework:

- a) Click  > **Cognos Analytics > Reporting Framework Generation**.
- b) Ensure that **All Models** is enabled, and then click **Submit**.

The framework models are published to Cognos Analytics in the Team content/<op_instance_name>/OpenPages Packages folder. The package name is OPENPAGES_REPORTS_V6.

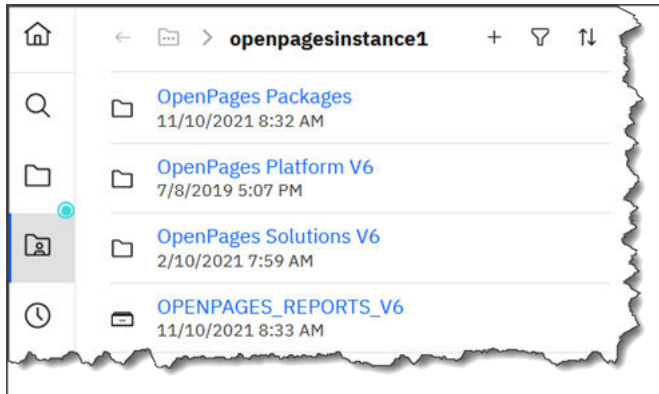


Figure 2. OpenPages integration folder in Cognos Analytics with reports and models

9. Verify the integration.

- Open the primary menu, and then click **Analytics**.
- Add a report to your dashboard, and then open the report.

Installing tools and utilities in Cloud Pak for Data

You can install tools and utilities, such as ObjectManager. You must run these tools and utilities from a remote system.

Before you begin

The computer where you install the tools and utilities must meet the following requirements:

- IBM SDK, Java Technology Edition 8 or Java Runtime Environment (JRE) 8 is installed.
- JAVA_HOME is defined.
- The remote system has access to IBM OpenPages for IBM Cloud Pak for Data.

About this task

Do this task if you want to use the following tools and utilities:

- ObjectManager: See Chapter 27, “The ObjectManager tool,” on page 881.
- chng-sys-password.sh: See [“Changing the password of the OPSysSystem user in IBM OpenPages for IBM Cloud Pak for Data”](#) on page 57.
- RpsRpF.sh: A command line tool for creating the reporting schema. See [“Generating the reporting schema and framework from a command line”](#) on page 164.

Procedure

1. Get the installation package.

- a. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

- b. Download the installation package:

```
oc cp openpages-<instance_name>-sts-0:/opt/ibm/OpenPages/openpages-tools.zip ./openpages-tools.zip
```

Replace *<instance_name>* with the name of the OpenPages instance.

2. Extract the `openpages-tools.zip` file to a new directory.
3. Go to the `openpages-tools/bin` directory.
4. Open the `openpages-tools.properties` file in a text editor.
5. Update the value of the `rest.url.path` property.
Type the base URL of the public REST API.

```
https://<cpd_url>/openpages-<instance_name>-grc
```

Replace *<cpd_url>* with the URL of IBM Cloud Pak for Data. Replace *<instance_name>* with the name of the OpenPages instance.

6. Set the value of the `platform.cloudpak.jwt.auth` property to `true`.
This setting enables you to authenticate by using either `jwt` and a IBM Cloud Pak for Data JSON Web Token (JWT) or your IBM Cloud Pak for Data username and API key rather than a username and password.
You generate the API key in IBM Cloud Pak for Data. For more information, see [Generating API keys for authentication](#).
7. By default, the application server's TLS (SSL) certificate is checked for validity when you run tools such as ObjectManager. To change this behavior, update the `insecure.skip.tls.verify` property.
For more information, see [“Tools properties and parameters” on page 1085](#).
8. Save and close the file.

Results

You can now run the tools by using the scripts and properties files in the `openpages-tools/bin` directory.

Configuring IBM OpenPages for IBM Cloud Pak for Data

You can configure IBM OpenPages for IBM Cloud Pak for Data to meet your business requirements. Some configuration tasks require you to do steps before and after making a change.

About this task

Do these tasks if you make any of the following configuration changes:

- Changes to WebSphere Liberty configuration files
- Changes to application configuration files
- Adding JAR files for custom triggers
- Adding custom JSPs, images, and CSS files

Preparing the instance

Do these steps to prepare your instance for configuration changes.

Procedure

1. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

2. Change to the project where OpenPages is installed:

```
oc project <Project>
```

3. If you use multiple replicas for the application server, scale down to a single replica.

```
oc scale --replicas=1 sts/openpages-<instance_name>-sts
```

To find the name of the StatefulSet (sts), run `oc get sts` and look for a name that starts with `openpages-`.

For example: `openpages-opinst-sts`

4. Log in to the application server pod and open a terminal.

```
oc exec -it openpages-<instance_name>-sts-0 -- /bin/bash
```

To find the pod name, run `oc get sts` and look for a name that starts with `openpages-`.

What to do next

Make your configuration changes, and then do the steps in [“Backing up changes and implementing them across replicas”](#) on page 46.

Backing up changes and implementing them across replicas

After you make configuration changes, do these steps to back up the configuration and implement the changes across application server replicas.

Procedure

1. Log in to the application server pod and open a terminal.

```
oc exec -it openpages-<instance_name>-sts-1 -- /bin/bash
```

To find the pod name, run `oc get sts` and look for a name that starts with `openpages-`.

2. Stop and then restart the application server.

```
server stop  
server start
```

3. Back up your IBM OpenPages for IBM Cloud Pak for Data configuration.

```
cd /opt/ibm/OpenPages/aurora/bin  
./OPBackup.sh /opt/ibm/OpenPages/openpages-backup-restore app-cp4d nosrvrst
```

A backup `.zip` file is created in `/opt/ibm/OpenPages/openpages-backup-restore`. The filename includes a timestamp.

The backup is restored automatically when you add more replicas or when the application server pod restarts (planned or unplanned restarts). The application server pod restart process uses the `.zip` file with the most recent timestamp.

4. Scale up to the number of replicas you want to use for the application server by running the following command:


```
oc scale --replicas=<#_of_replicas> sts/openpages-<instance_name>-sts
```

Replace the following values:

Variable	Replace with
<#_of_replicas>	Specify the number of replicas. Can be 1 or more.
<statefulset_name>	Specify the name of the StatefulSet for the application. To find the name of the StatefulSet, run <code>oc get sts</code> and look for a name that starts with <code>openpages-</code> . For example, <code>openpages-opinst-sts</code>

Backing up IBM OpenPages for IBM Cloud Pak for Data

You can back up your IBM OpenPages for IBM Cloud Pak for Data instance.

This topic describes backing up instances of IBM OpenPages for IBM Cloud Pak for Data for Refresh 1 of Cloud Pak for Data Version 4.0 and earlier versions.

For Refresh 2 of Cloud Pak for Data Version 4.0, released in October 2021, see [Backing up and restoring an entire deployment with the Cloud Pak for Data OADP backup and restore service](#) and, if you encounter issues while backing up or restoring, see [Troubleshooting OpenPages backup and restore](#).

Before you begin

If you have custom JSPs or other custom files, you need to do some additional steps before you run a backup. For more information, see [“Backing up custom files in IBM OpenPages for IBM Cloud Pak for Data” on page 50](#).

If you use custom keystores, ensure that the keystore files are stored in `/opt/ibm/wlp/output/defaultServer/resources/security`. Or, add the keystore files to the `/opt/ibm/OpenPages/aurora/bin/op-backup.manifest` file.

About this task

When you back up IBM OpenPages for IBM Cloud Pak for Data, you need to back up both the database and the application files. The application files include the `openpages-storage` directory, which contains file attachments, and the application configuration.

You can do an online backup or an offline backup.

- [“Performing an online backup” on page 47](#)
- [“Performing an offline backup” on page 49](#)

For information about backing up external databases for IBM OpenPages for IBM Cloud Pak for Data, see [Backing up, restoring, and migrating OpenPages](#).

Performing an online backup

Do an online backup when you want to back up IBM OpenPages for IBM Cloud Pak for Data without restarting the servers.

Procedure

1. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

2. Change to the project where OpenPages is installed:

```
oc project <Project>
```

3. Log in to the database server pod.

Do one of the following steps:

- Run the following command:

```
oc exec -it c-db2oltp-*>-db2u-0 -- /bin/bash
```

To find the name of the pod, run `oc get sts` and look for a name with the pattern `c-db2oltp-*-db2u-0`.

For example, `c-db2oltp-1601355983782494-db2u-0`

- Or, in the Red Hat OpenShift console, go to the Db2 server pod and open a terminal.

4. Switch to the `db2inst1` user by running the following command:

```
su - db2inst1
```

5. Verify that the database parameter `LOGARCHMETH1` is configured

Run the following command:

```
db2 get db cfg for OPX | grep LOGARCHMETH1
```

Look for a result that is similar to the following text:

```
First log archive method
(LOGARCHMETH1) = DISK:/mnt/bludata0/db2/archive_log/
```

6. Back up the database by running the following command:

```
db2 backup db OPX on all dbpartitionnums online to /mnt/backup include logs without prompting
```

An encrypted backup is created in the `/mnt/backup` directory, which is a persistent storage volume.

7. Log in to any of the application server pods.

Use one of the following methods:

Using the web client

In the Red Hat OpenShift console, go to an application server pod and open a terminal.

Using the command line

- a. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

- b. Change to the project where the IBM Cloud Pak for Data control plane is installed:

```
oc project <Project>
```

- c. Log in to the application server pod and open a terminal:

```
oc exec -it openpages-<instance_name>-sts-<N> -- /bin/bash
```

To find the pod name, run `oc get sts` and look for a name that starts with `openpages-`.

8. Back up OpenPages by running the following command:

```
cd /opt/ibm/OpenPages/aurora/bin
./OPBackup.sh nosrvist
```

The backup is created in the `/opt/ibm/OpenPages/openpages-backup-restore` directory, which is a persistent storage volume. The runtime data in the backup is encrypted. The backup also contains configuration customizations.

Performing an offline backup

Procedure

1. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

2. Change to the project where OpenPages is installed:

```
oc project <Project>
```

3. Scale down to 0 replicas.

```
oc scale --replicas=0 sts/openpages-<instance_name>-sts
```

To find the name of the StatefulSet (sts), run `oc get sts` and look for a name that starts with `openpages-`. For example, `openpages-instance_name-sts`

4. If you are using an external database, back up the database by using the steps in [“Db2 database backup and restore for OpenPages”](#) on page 690, and then continue with step “8” on page 49.

5. Log in to the database server pod.

Do one of the following steps:

- Run the following command:

```
oc exec -it c-db2oltp-<*>-db2u-0 -- /bin/bash
```

To find the name of the pod, run `oc get sts` and look for a name with the pattern `c-db2oltp-*db2u-0`.

For example, `c-db2oltp-1601355983782494-db2u-0`

- Or, in the Red Hat OpenShift console, go to the Db2 server pod and open a terminal.

6. Switch to the `db2inst1` user by running the following command:

```
su - db2inst1
```

7. Back up the database.

Do the steps in the following task, starting at step 4 (offline backup): [Backing up a Db2 database](#).

- Replace the database name `BLUDB` with `OPX`.
- Replace `backup_dir` with `/mnt/backup`

An encrypted backup is created in the `/mnt/backup` directory, which is a persistent storage volume.

8. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

9. Change to the project where OpenPages is installed:

```
oc project <Project>
```

10. Scale to 1 replica.

```
oc scale --replicas=1 sts/openpages-<instance_name>-sts
```

To find the name of the StatefulSet (sts), run `oc get sts` and look for a name that starts with `openpages-`. For example, `openpages-opinst-sts`

11. When the application server pod is ready, log in to the pod.

Use one of the following methods:

Using the web client

In the Red Hat OpenShift console, go to an application server pod and open a terminal.

Using the command line

- a. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

- b. Change to the project where the IBM Cloud Pak for Data control plane is installed:

```
oc project <Project>
```

- c. Log in to the application server pod and open a terminal:

```
oc exec -it openpages-<instance_name>-sts-0 -- /bin/bash
```

To find the pod name, run `oc get sts` and look for a name that starts with `openpages-`.

12. Back up OpenPages by running the following command:

```
cd /opt/ibm/OpenPages/aurora/bin
./OPBackup.sh
```

The backup is created in the `/opt/ibm/OpenPages/openpages-backup-restore` directory, which is a persistent storage volume. The runtime data in the backup is encrypted. The backup also contains configuration customizations.

13. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

14. Change to the project where OpenPages is installed:

```
oc project <Project>
```

15. Scale up to the number of replicas you want to use for the application server by running the following command:

```
oc scale --replicas=<#_of_replicas> sts/openpages-<instance_name>-sts
```

Replace the following values:

Variable	Replace with
<#_of_replicas>	Specify the number of replicas. Can be 1 or more.
<statefulset_name>	Specify the name of the StatefulSet for the application. To find the name of the StatefulSet, run <code>oc get sts</code> and look for a name that starts with <code>openpages-</code> . For example, <code>openpages-opinst-sts</code>

Backing up custom files in IBM OpenPages for IBM Cloud Pak for Data

You can include custom files, such as custom JSPs or other files that are specific to your environment, in backups by using a manifest file. A manifest file is a text file that contains the full path name to any directory or file that needs to be included in the backup.

For example, if you want to back up `openpages-ext.jar`, add its full path to the manifest file:

```
/opt/ibm/OpenPages/aurora/lib/openpages-ext.jar
```

Before you begin

- You must list all of your custom directories and files in a manifest. If you have any questions about the location of your custom data, contact IBM OpenPages Support.

Procedure

1. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

2. Change to the project where OpenPages is installed:

```
oc project <Project>
```

3. If you use multiple replicas for the application server, scale down to a single replica.

```
oc scale --replicas=1 sts/openpages-<instance_name>-sts
```

To find the name of the StatefulSet (sts), run `oc get sts` and look for a name that starts with `openpages-`.

For example: `openpages-opinst-sts`

4. Log in to the application server pod.

- a) Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

- b) Change to the project where the IBM Cloud Pak for Data control plane is installed:

```
oc project <Project>
```

- c) Log in to the application server pod and open a terminal:

```
oc exec -it openpages-<instance_name>-sts-0 -- /bin/bash
```

To find the pod name, run `oc get sts` and look for a name that starts with `openpages-`.

5. If you have custom JSPs, do the following steps:

- a) Create a zip file called `solutions-sosa-files.zip` that contains your custom JSPs and related files.

Tip: You can use a different name, but it must follow the convention `*-sosa-files.zip`. Also, you must add it to the `<OP_HOME>/aurora/bin/op-backup.manifest` file. Only `solutions-sosa-files.zip` is backed up and restored by default.

- b) Put the `solutions-sosa-files.zip` file in the `<OP_HOME>/applications` directory.

- When you run `OPBackup`, the zip file is included in the backup.
- When you run `OPRestore`, the zip file is restored to `<OP_HOME>/applications` and is also extracted to `/opt/ibm/wlp/usr/servers/defaultServer/apps/expanded/op-apps.ear/taskui.war/`

6. Open the `<OP_HOME>/aurora/bin/op-backup.manifest` file in a text editor.

7. Add custom files or directories, other than JSPs, to the `op_backup.manifest` file.

You can specify directories or individual files. For each file or directory, create a new line and type its full path..

8. Save the manifest file using the current location and name.

9. Stop and then restart the application server.

```
server stop  
server start
```

10. Back up your IBM OpenPages for IBM Cloud Pak for Data configuration.

For more information, see [“Backing up IBM OpenPages for IBM Cloud Pak for Data” on page 47.](#)

Restoring IBM OpenPages for IBM Cloud Pak for Data

You can restore a backup of your IBM OpenPages for IBM Cloud Pak for Data instance.

This topic describes restoring backed up instances of IBM OpenPages for IBM Cloud Pak for Data for Refresh 1 of Cloud Pak for Data Version 4.0 and earlier versions.

For Refresh 2 of Cloud Pak for Data Version 4.0, released in October 2021, see [Backing up and restoring an entire deployment with the Cloud Pak for Data OADP backup and restore service](#) and, if you encounter issues while backing up or restoring, see [Troubleshooting OpenPages backup and restore](#).

About this task

Use these steps to restore the instance that you backed up. If you want to restore the backup into a different instance, see [“Migrating IBM OpenPages for IBM Cloud Pak for Data to another instance” on page 54.](#)

Procedure

1. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

2. Change to the project where OpenPages is installed:

```
oc project <Project>
```

3. Scale down to 0 replicas.

```
oc scale --replicas=0 sts/openpages-<instance_name>-sts
```

To find the name of the StatefulSet (sts), run `oc get sts` and look for a name that starts with `openpages-`. For example, `openpages-instance_name-sts`

4. If you are using an external database, restore the database by using the steps in [“Db2 database backup and restore for OpenPages” on page 690](#), and then continue with step [“7” on page 52.](#)
5. Log in to the database server pod.

Do one of the following steps:

- Run the following command:

```
oc exec -it c-db2oltp-<*>-db2u-0 -- /bin/bash
```

To find the name of the pod, run `oc get sts` and look for a name with the pattern `c-db2oltp-*-db2u-0`.

For example, `c-db2oltp-1601355983782494-db2u-0`

- Or, in the Red Hat OpenShift console, go to the Db2 server pod and open a terminal.

6. Restore the database.

Do the steps in the following task: [Restoring a Db2 database.](#)

- Replace the database name BLUDB with OPX.
- Replace `backup_dir` with `/mnt/backup`

7. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

8. Change to the project where OpenPages is installed:

```
oc project <Project>
```

9. Scale to 1 replica.

```
oc scale --replicas=1 sts/openpages-<instance_name>-sts
```

To find the name of the StatefulSet (sts), run `oc get sts` and look for a name that starts with `openpages-`. For example, `openpages-opinst-sts`

10. Log in to the application server pod and open a terminal.

```
oc exec -it openpages-<instance_name>-sts-0 -- /bin/bash
```

To find the pod name, run `oc get sts` and look for a name that starts with `openpages-`.

11. Go to the `/opt/ibm/OpenPages/openpages-backup-restore` directory.
12. Locate the backup file that has the most recent timestamp. Use this file in step “13” on page 53.
13. Restore the backup by running the following commands:

```
cd /opt/ibm/OpenPages/aurora/bin  
./OPRestore.sh <backup_filename_without_the_file_extension>
```

For example:

```
cd /opt/ibm/OpenPages/aurora/bin  
./OPRestore.sh op_backup_2020_11_20_21_43_04
```

14. Restart the application server by running the following command:

```
server start
```

15. Go to the `/opt/ibm/OpenPages/openpages-backup-restore` directory. Move all backup files, except the file you used in step “13” on page 53, to a subfolder under `/opt/ibm/OpenPages/openpages-backup-restore`.
16. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

17. Change to the project where OpenPages is installed:

```
oc project <Project>
```

18. Scale up to the number of replicas you want to use for the application server by running the following command:

```
oc scale --replicas=<#_of_replicas> sts/openpages-<instance_name>-sts
```

Replace the following values:

Variable	Replace with
<#_of_replicas>	Specify the number of replicas. Can be 1 or more.
<statefulset_name>	Specify the name of the StatefulSet for the application. To find the name of the StatefulSet, run <code>oc get sts</code> and look for a name that starts with <code>openpages-</code> . For example, <code>openpages-opinst-sts</code>

Migrating IBM OpenPages for IBM Cloud Pak for Data to another instance

You can migrate IBM OpenPages for IBM Cloud Pak for Data from one instance to another.

This topic describes migrating instances of IBM OpenPages for IBM Cloud Pak for Data for Refresh 1 of Cloud Pak for Data Version 4.0 and earlier versions.

For Refresh 2 of Cloud Pak for Data Version 4.0, released in October 2021, see [Backing up and restoring an entire deployment with the Cloud Pak for Data OADP backup and restore service](#) and, if you encounter issues while backing up or restoring, see [Troubleshooting OpenPages backup and restore](#).

Procedure

1. In your source environment, log in to your OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

2. Change to the project where OpenPages is installed:

```
oc project <Project>
```

3. Back up the encryption keys and secrets in the source environment.

Do these steps so that the backup files can be decrypted in the target environment and so that the target environment has the same secrets as the source environment.

- a) Log in to the database server pod.

Do one of the following steps:

- Run the following command:

```
oc exec -it c-db2oltp-*>-db2u-0 -- /bin/bash
```

To find the name of the pod, run `oc get sts` and look for a name with the pattern `c-db2oltp-*-db2u-0`.

For example, `c-db2oltp-1601355983782494-db2u-0`

- Or, in the OpenShift console, go to the Db2 server pod and open a terminal.

- b) Switch to the `db2inst1` user by running the following command:

```
su - db2inst1
```

- c) Locate the encryption keys by running the following command:

```
gsk8capicmd_64 -cert -list -db /mnt/blumeta0/db2/keystore/keystore.p12 -stashed
```

Look for a result that is similar to the following text:

```
* default, - personal, ! trusted, # secret key
#      DB2_SYSGEN_db2inst1_OPX_2020-10-19-17.51.55_81D83D47
#      DB2_SYSGEN_db2inst1_OPX_2020-10-19-17.56.05_AF8AC2F5
```

- d) Extract the keys from the keystore by running the following command:

```
gsk8capicmd_64 -secretkey -extract -db /mnt/blumeta0/db2/keystore/keystore.p12
-stashed -target <label>.sec -format pkcs12 -label <label>
```

- e) Note the `<label>` of each key. You need this information later.

4. Run the following commands. Note the secret that is returned by each command. You need this information later.

```
oc get secret openpages-instance_name-platform-secret -o jsonpath="{.data.encryption-key-pw}"
oc get secret openpages-instance_name-platform-secret -o jsonpath="{.data.keystore-pw}"
```



```
oc get secret openpages-instance_name-platform-secret -o jsonpath="{.data.ldap-search-pw}"
oc get secret openpages-instance_name-platform-secret -o jsonpath="{.data.opsystem-pw}"
```

In addition, you can migrate the initial secrets for the out-of-the-box user accounts. Do this, for example, if you did not change the initial password of a user account and you want to migrate the initial secret to your new instance. To get the secret, run the following command for each secret that you want to migrate:

```
oc get secret openpages-instance_name-initialpw-secret -o jsonpath="{.data.<user name>}"
```

Replace the following values:

Variable	Replace with
<i><instance_name></i>	The name of your OpenShift instance.
<i><user name></i>	A user account

The encoded password of the account is displayed. Save the password.

5. Back up your source environment by doing an offline backup. See [“Performing an offline backup” on page 49](#).
6. Copy the backup files to the target environment.
 - Copy the database backup to the `/mnt/backup` directory in the database server pod.
 - Copy the extracted encryption key files to the database server pod.
 - Copy the `op_backup_<timestamp>.zip` file from step “5” on [page 55](#) to one of the application server pods and place it in the `/opt/ibm/OpenPages/openpages-backup-restore` directory.
 - Move all other `op_backup_<timestamp>.zip` files to a subfolder under `/opt/ibm/OpenPages/openpages-backup-restore`.

7. In your target environment, log in to your OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

8. Change to the project where OpenPages is installed:

```
oc project <Project>
```

9. Import the encryption keys to the target environment.

- a) Log in to the database server pod.

Do one of the following steps:

- Run the following command:

```
oc exec -it c-db2oltp-<*>-db2u-0 -- /bin/bash
```

To find the name of the pod, run `oc get sts` and look for a name with the pattern `c-db2oltp-<*>-db2u-0`.

For example, `c-db2oltp-1601355983782494-db2u-0`

- Or, in the OpenShift console, go to the Db2 server pod and open a terminal.

- b) Switch to the `db2inst1` user by running the following command:

```
su - db2inst1
```

- c) Import the encryption keys by running the following command for each key:

The *<label>* must match the *<label>* from the source environment.

```
gsk8capicmd_64 -secretkey -add -db /mnt/blumeta0/db2/keystore/keystore.p12
-stashed -label <label> -format pkcs12 -file <key file path>
```

For example:

```
gsk8capicmd_64 -secretkey -add -db /mnt/blumeta0/db2/keystore/keystore.p12
-stashed -label DB2_SYSGEN_db2inst1_OPX_2020-10-12-20.09.20_9F1D9078
-format pkcs12 -file /tmp/seckey/DB2_SYSGEN_db2inst1_OPX_2020
-10-12-20.09.20_9F1D9078.sec
```

10. Scale to 1 replica.

```
oc scale --replicas=1 sts/openpages-<instance_name>-sts
```

To find the name of the StatefulSet (sts), run `oc get sts` and look for a name that starts with `openpages-`. For example, `openpages-opinst-sts`

11. Log in to the application server pod and open a terminal.

```
oc exec -it openpages-<instance_name>-sts-0 -- /bin/bash
```

To find the pod name, run `oc get sts` and look for a name that starts with `openpages-`.

12. Go to the `/opt/ibm/OpenPages/openpages-backup-restore` directory.
13. Locate the `op_backup_<timestamp>.zip` file that you copied from your source environment. Use this file in step “14” on page 56.
14. Restore the backup by running the following commands:

```
cd /opt/ibm/OpenPages/aurora/bin
./OPRestore.sh <backup_filename_without_the_file_extension>
```

For example:

```
cd /opt/ibm/OpenPages/aurora/bin
./OPRestore.sh op_backup_2021_01_20_21_43_04
```

15. Stop the application server pods.

- a) Scale down to 0 replicas.

```
oc scale --replicas=0 sts/openpages-<instance_name>-sts
```

To find the name of the StatefulSet (sts), run `oc get sts` and look for a name that starts with `openpages-`. For example, `openpages-instance_name-sts`

- b) Wait until all application server pods are deleted.

16. Log in to the database server pod.

Do one of the following steps:

- Run the following command:

```
oc exec -it c-db2oltp-<*>-db2u-0 -- /bin/bash
```

To find the name of the pod, run `oc get sts` and look for a name with the pattern `c-db2oltp-*db2u-0`.

For example, `c-db2oltp-1601355983782494-db2u-0`

- Or, in the Red Hat OpenShift console, go to the Db2 server pod and open a terminal.

17. Restore the database.

Do the steps in the following task: [Restoring a Db2 database](#).

- Replace the database name BLUDB with OPX.
- Replace `backup_dir` with `/mnt/backup`

For more information, see [Restoring an encrypted backup image to a different system with a local key manager](#)

18. Restore the secrets into the target environment.

- a) Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

- b) Change to the project where OpenPages is installed:

```
oc project <Project>
```

- c) Run the following command:

```
oc edit secrets openpages-<instance_name>-platform-secret
```

- d) Update the values for each secret based on the values in your source environment.

For more information, see [Secrets](#) in the Kubernetes documentation.

- e) If you want to restore the initial secrets for the out-of-the-box user accounts, run the following command:

```
oc edit secrets openpages-<instance_name>-initialpw-secret
```

Do this, for example, if you did not change the initial password of an out-of-the-box user account and you want to migrate the account's initial secret from your old instance to your new instance.

19. Scale up to the number of replicas you want to use for the application server by running the following command:

```
oc scale --replicas=<#_of_replicas> sts/openpages-<instance_name>-sts
```

Replace the following values:

Variable	Replace with
<#_of_replicas>	Specify the number of replicas. Can be 1 or more.
<statefulset_name>	Specify the name of the StatefulSet for the application. To find the name of the StatefulSet, run <code>oc get sts</code> and look for a name that starts with <code>openpages-</code> . For example, <code>openpages-opinst-sts</code>

Changing the password of the OPSys user in IBM OpenPages for IBM Cloud Pak for Data

You can change the password of the OPSys user. OPSys is a default service user account that is required by internal system actions.

Before you begin

The `chng-sys-pswd` tool must be installed on a remote system that can access the OpenPages URL. For more information, see [“Installing tools and utilities \(IBM OpenPages with Watson\)”](#) on page 824.

Procedure

1. Log in to the Red Hat OpenShift web client as an administrator.
2. Click **Workload** > **Secrets**, and then click **openpages-<instance_name>-platform-secret**.
3. Find the value for **opsystem-pw**.
The value in **opsystem-pw** is the current password of the OPSys user. You need this password in a later step.
4. Log in to the remote system where you installed the OpenPages tools and utilities.

5. Go to the `openpages-tools-client/bin` directory.
6. Run the following command:

```
chng-sys-pswd.sh
```

7. Follow the prompts to set the new password.

Important: You must respond to the authentication prompts using one of the following options:

- If you respond to the prompt **Enter 'jwt' or CP4D user name:** with `jwt`, you must respond to the prompt **Enter Json Web Token or CP4D API Key:** with a JSON Web Token.
- If you respond to the prompt **Enter 'jwt' or CP4D user name:** with your Cloud Pak for Data user name, you must respond to the prompt **Enter Json Web Token or CP4D API Key:** with your Cloud Pak for Data API key.

An API Key can be generated in Cloud Pak for Data. For more information, see [Generating API keys for authentication](#).

8. Make a note of the password. You will need it in a later step.
The script asks you to restart the services. Skip this step. You restart the services in a later step.
9. Return to the Red Hat OpenShift web client and log in as an administrator.
10. Click **Workload > Pods**, and then click **openpages-<instance_name>-sts-0**.
11. Click **Terminal**.
12. Back up the configuration by running the following command:

```
cd /opt/ibm/OpenPages/aurora/bin  
./OPBackup.sh /opt/ibm/OpenPages/openpages-backup-restore app-cp4d nosrvrst
```

The backup is created in the `/opt/ibm/OpenPages/openpages-backup-restore` directory.

13. Click **Workload > Secrets**, and then click **openpages-<instance_name>-platform-secret**.
14. Click **Actions > Edit Secret**.
15. Update **opsystem-pw** with the new OPSys password.
16. Restart the application server pods.
 - a) Click **Workload > StatefulSets**, and then click **openpages-<instance_name>-sts**.
 - b) Decrease the number of pods to 0. Wait for all pods to be removed.
 - c) Increase the number of pods to the value that you use in your environment.

Changing the password of the Liberty keystore in IBM OpenPages for IBM Cloud Pak for Data

You can change the password of the IBM WebSphere Liberty keystore.

Procedure

1. Log in to the Red Hat OpenShift web client as an administrator.
2. Click **Workload > Secrets**, and then click **openpages-<instance_name>-platform-secret**.
3. Find the value for **keystore-pw**.
The value in **keystore-pw** is the current password of the keystore. You need this password in a later step.
4. Click **Workload > Pods**, and then click **openpages-<instance_name>-sts-0**.
5. Click **Terminal**.
6. Run the following command:

```
keytool -storepasswd -keystore /opt/ibm/wlp/output/defaultServer/resources/security/key.p12  
-storetype PKCS12 -storepass <current_password>
```

Replace `<current_password>` with the current password of the keystore.

7. Follow the prompts to set the new password.

Make a note of the password. You need it in a later step.

8. Back up the configuration by running the following command:

```
cd /opt/ibm/OpenPages/aurora/bin
./OPBackup.sh /opt/ibm/OpenPages/openpages-backup-restore app-cp4d nosivrst
```

The backup is created in the `/opt/ibm/OpenPages/aurora/openpages-backup-restore` directory.

9. Return to the Red Hat OpenShift web client.

10. Click **Workload** > **Secrets**, and then click **openpages-<instance_name>-platform-secret**.

11. Click **Actions** > **Edit Secret**.

12. Update **keystore-pw** with the new keystore password.

13. Restart the application server pods.

- Click **Workload** > **StatefulSets**, and then click **openpages-<instance_name>-sts**.
- Decrease the number of pods to 0. Wait for all pods to be removed.
- Increase the number of pods to the value that you use in your environment.

Results

The keystore password is changed. To verify the change, do the following steps:

1. Click **Workload** > **Pods**, and then click **openpages-<instance_name>-sts-0**.

2. Click **Terminal**.

3. Run the following command:

```
keytool -list -keystore /opt/ibm/wlp/output/defaultServer/resources/security/key.p12
-storetype PKCS12 -storepass <new_password>
```

Where `<new_password>` is the password that you set in step “7” on page 59.

Configuring server certificates in IBM OpenPages for IBM Cloud Pak for Data

You can configure the server certificates that are used by IBM OpenPages for IBM Cloud Pak for Data.

About this task

By default, OpenShift uses a self-signed wildcard certificate for applications within a cluster. You can replace the default certificate by using one of the following approaches:

- Replace the self-signed certificate for your entire cluster with a wildcard certificate from a certificate authority (CA)
- Or, set up CA certificate only for your OpenPages instance

Replacing the self-signed certificate for the cluster

With this option, you replace the self-signed certificate with a wildcard certificate from a certificate authority (CA). The wildcard certificate is used for the entire OpenShift cluster where IBM Cloud Pak for Data is installed. The certificate is used for all applications in the cluster, including OpenPages.

Before you begin

To use this option, you must have a wildcard certificate from your CA.

About this task

For more information, see [Replacing the default ingress certificate](#) in the OpenShift documentation.

Setting up a CA certificate for OpenPages

With this option, you set up CA certificate only for your OpenPages instance.

Before you begin

To use this option, you must meet the following requirements:

- You have a running OpenPages instance.
- You have a valid certificate, root certificate, and (optionally) an intermediate certificate.
- All certificates are in .pem Base64 format.

For more information, see [Secured routes](#) in the OpenShift documentation.

Procedure

1. If you are using an intermediate certificate, concatenate the root and intermediate certificates.
For example:

```
cat carootcert.pem caintermediatecert.pem > cacert.pem
```

2. Edit the OpenPages route.

Run the following command:

```
oc edit route/openpages-<instance_name>
```

Add the contents of the .pem and .key files to the route definition file.

Note: Modify only these three fields: `spec.tls.certificate`, `spec.tls.key`, and `spec.tls.caCertificate`.

The file must be well-formed YAML. Ensure that the content that you paste into the file is indented correctly, as shown in this example:

```
spec:
  tls:
    termination: reencrypt
    certificate: |-
      -----BEGIN CERTIFICATE-----
      COPY CONTENTS OF YOUR CERTIFICATE (cert.pem) HERE
      -----END CERTIFICATE-----
    key: |-
      -----BEGIN PRIVATE KEY-----
      COPY CONTENTS OF your .key file here
      -----END PRIVATE KEY-----
    caCertificate: |-
      -----BEGIN CERTIFICATE-----
      COPY CONTENTS OF THE CERTIFICATE FROM STEP 1 (cacert.pem) HERE
      -----END CERTIFICATE-----
```

Importing a certificate into the local trust store on IBM OpenPages for IBM Cloud Pak for Data

Use the following steps to import certificates. A certificate is needed to build a secure connection between IBM OpenPages for IBM Cloud Pak for Data and third-party servers, such as regulatory feed providers.

About this task

If you want to import data from a regulatory provider, such as Ascent Reg Tech, Reg-Track, Thomson Reuters Regulatory Intelligence, or Wolters Kluwer, you need to import a certificate to set up a secure connection.

Procedure

1. Get the keystore password.
 - a) Log in to the Red Hat OpenShift web client as an administrator.
 - b) Click **Workload > Secrets**, and then click **openpages-<instance_name>-platform-secret**.
 - c) Find the value for **keystore-pw**. You need this password in a later step.
2. Get the certificates from the regulatory feed provider and place them in a directory called `certs`.
3. Copy the `certs` directory to the `openpages-<instance_name>-sts-0` pod.

```
oc rsync certs openpages-<instance_name>-0:/openpages-shared
```

4. Do the steps in “Preparing the instance” on page 46.
5. In the `openpages-<instance_name>-sts-0` pod, go to the `openpages-shared/certs` directory.
6. If you're replacing a certificate, delete any existing certificates for the regulatory feed provider.

```
keytool -delete -alias <CERTIFICATE_ALIAS> -keystore /output/resources/security/key.p12  
-storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- `<CERTIFICATE_ALIAS>` is the alias of the existing certificate of the feed provider.
- `<STORE_PASSWORD>` is the password of the trust store on the application server, which you retrieved in “1” on page 61.

7. Import the certificate to WebSphere Liberty by running the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_FILE_NAME> -keystore /  
output/resources/security/key.p12 -storetype PKCS12 -storepass <STORE_PASSWORD> -noprompt
```

Where:

- `<CERTIFICATE_ALIAS>` is the alias of the certificate of the feed provider.
- `<CERTIFICATE_FILE_NAME>` is the file name of the certificate.
- `<STORE_PASSWORD>` is the password of the trust store on the application server, which you retrieved in “1” on page 61.

For more information about `keytool`, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

8. Do the steps in “Backing up changes and implementing them across replicas” on page 46.
9. Optional: Remove the `certs` directory.

```
rm -rf /openpages-shared/certs
```

Changing the data encryption key for IBM OpenPages for IBM Cloud Pak for Data

You can change the encryption key that is used to encrypt data in IBM OpenPages for IBM Cloud Pak for Data.

Before you begin

Before you do this task, review the following prerequisites:

- You are familiar with encryption keys and how to manage them.
- You know how to use the OpenPages GRC REST API or you have experience with other REST APIs.
- You can log in to the OpenPages application as a super administrator, such as OpenPagesAdministrator.
- You can log in to Red Hat OpenShift as a project administrator.

About this task

Do the following tasks in order:

1. [“Backing up the current encryption key” on page 62](#)
2. [“Backing up OpenPages” on page 63](#)
3. [“Decrypting data with the current encryption key” on page 63](#)
4. [“Generating a new secret key” on page 64](#)
5. [“Updating OpenShift with the new key” on page 64](#)
6. [“Restarting the application servers” on page 65](#)
7. [“Encrypting data with the new key” on page 65](#)
8. [“Restarting the application servers” on page 66](#)

Backing up the current encryption key

Back up your current encryption key.

Procedure

1. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

2. Change to the project where OpenPages is installed:

```
oc project <Project>
```

3. Retrieve the current encryption key by running the following command:

```
oc get secret openpages-<instance name>-platform-secret -o jsonpath="{.data.encryption-key-pw}"
```

The command returns the base64 encoded key that is used currently for data encryption in your instance.

Save the key in a secure location. You might need it later, for example if you need to restore a backup.

Backing up OpenPages

Back up your OpenPages instance.

About this task

You can do an online backup or an offline backup. For more information, see [“Backing up IBM OpenPages for IBM Cloud Pak for Data” on page 47](#).

Decrypting data with the current encryption key

After you complete the backups, decrypt the data by using the current encryption key so that you can encrypt the data later with a new key.

Before you begin

To do this task, the application pods must be in a **Running** state and their readiness status must be **Ready**.

About this task

Use the following OpenPages GRC REST API endpoint to decrypt the data:

```
https://<op_app_server>:<op_port>/grc/api/configuration/decryptWithExternalKey
```

To call the API, send an `https` PUT request to the path by using an HTTPS client. You can use a `curl` command, for example:

```
curl -k --location --request PUT --header 'Content-Type: application/json'
--header 'Accept: application/json' -u <op_super_user>:<op_super_user_password>
'https://<op_app_server>:<op_port>/grc/api/configuration/decryptWithExternalKey'
```

The API response includes the process ID of the decryption long running process, for example `{"processId": "2927"}`

Note the following details about the `curl` command:

- The `-u` parameter requires an OpenPages username and password. This user must be an OpenPages super administrator, such as `OpenPagesAdministrator`.
- The `-k` parameter allows connections to SSL sites without trusted certificates. This parameter is not needed if you replaced the default certificates with your own certificate authority (CA)-signed certificates.

You can check the status of the decryption process by using the following API:

```
https://<op_app_server>:<op_port>/grc/api/processes/<process_Id>
```

You can call the API by using your browser or by using an HTTPS client to send a GET request.

For example:

```
curl -k --location -u <op_super_user>:<op_super_user_password>
--header 'Content-Type: application/json' --header 'Accept: application/json'
--request GET 'https://<op_app_server>:<op_port>/grc/api/processes/<process_Id>'
```

In the response, the status attribute indicates whether the process is finished or still in progress. You can repeat the check as needed. The process is complete when the status value is `STATUS_FINISHED_SUCCESS`.

The decryption process can take time, depending on the data volume. It takes longer especially if you have many file attachment records.

To check the logs for a process, you can send a GET request to the following endpoint:

```
https://<op_app_server>:<op_port>/grc/api/processes/<process_Id>/logs
```

Generating a new secret key

Generate a new encryption key.

About this task

IBM OpenPages for IBM Cloud Pak for Data uses AES256 for data encryption. The key must be 256 bits (32 bytes) in length and it must be encoded with base64. The key must meet these requirements so it can be stored in a Kubernetes secret.

Note: A 256-bit key that is encoded with base64 is 44 characters in length.

To generate a new random key, you can use a random generation tool or you can use `openssl`. The `openssl` command is available on the OpenPages application server pod:

Important: In either case, save the key value in a secure location. The key value will be stored only in Kubernetes Secrets. The key value is not persisted by OpenPages and the key value cannot be recovered if it's lost.

Procedure

1. Log in to the application server pod and open a terminal window.

Use one of the following methods:

Using the web client

In the Red Hat OpenShift console, go to an application server pod and open a terminal.

Using the command line

- a. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

- b. Change to the project where the IBM Cloud Pak for Data control plane is installed:

```
oc project <Project>
```

- c. Log in to the application server pod and open a terminal:

```
oc exec -it openpages-<instance_name>-sts-1 -- /bin/bash
```

To find the pod name, run `oc get sts` and look for a name that starts with `openpages-`.

2. Run the following command to create the key:

```
openssl rand -base64 32 | head -c24 | tr -d '\n' | base64
```

3. Save the new key value in a secure location.

Updating OpenShift with the new key

Update the Kubernetes Secret in OpenShift with the new key value.

Procedure

1. Open the Red Hat OpenShift web client.
2. Click **Workload** > **Secrets**, and then click **openpages-<instance_name>-platform-secret**.
3. Click **Actions** > **Edit Secret**.
4. Update **encryption-key-pw** with the new base64 encoded key value.

Tip: You can also update the key value by using the command line. Run `oc edit secrets openpages-<instance_name>-platform-secret`. In the yaml file, update `encryption-key-pw` with the new base64 encoded key value.

Restarting the application servers

Restart the application server pods and scale up to the number of replicas you want to use.

Procedure

1. Scale down to 0 replicas.

```
oc scale --replicas=0 sts/openpages-<instance_name>-sts
```

To find the name of the StatefulSet (sts), run `oc get sts` and look for a name that starts with `openpages-`. For example, `openpages-<instance_name>-sts`

2. Wait until all application server pods are deleted.
3. Scale up to the number of replicas you want to use for the application server by running the following command:

```
oc scale --replicas=<#_of_replicas> sts/openpages-<instance_name>-sts
```

Replace the following values:

Variable	Replace with
<code><#_of_replicas></code>	Specify the number of replicas. Can be 1 or more.
<code><statefulset_name></code>	Specify the name of the StatefulSet for the application. To find the name of the StatefulSet, run <code>oc get sts</code> and look for a name that starts with <code>openpages-</code> . For example, <code>openpages-opinst-sts</code>

Encrypting data with the new key

You are now ready to encrypt the data with the new encryption key.

Before you begin

To do this task, the application pods must be in a **Running** state and their readiness status must be **Ready**.

About this task

Use the following OpenPages GRC REST API endpoint to encrypt the data:

```
https://<op_app_server>:<op_port>/grc/api/configuration/encryptWithExternalKey
```

To call the API, send an `https PUT` request to this path by using an HTTPS client. You can use a `curl` command, for example:

```
curl -k --location --request PUT --header 'Content-Type: application/json'
--header 'Accept: application/json' -u <super user>:<password> --cookie-jar cookie-jar.txt
--cookie cookie-jar.txt 'https://<op_app_server>:<op_port>/grc/api/configuration/
encryptWithExternalKey'
```

The API response includes the process ID of the encryption long running process, for example `{"processId": "2928"}`

Note the following details about the `curl` command:

- The `-u` parameter requires an OpenPages username and password. This user must be an OpenPages super administrator, such as `OpenPagesAdministrator`.
- The `-k` parameter allows connections to SSL sites without trusted certificates. This parameter is not needed if you replaced the default certificates with your own certificate authority (CA)-signed certificates.

You can check the status of the encryption process by using the following API:

```
https://<op_app_server>:<op_port>/grc/api/processes/<process_Id>
```

You can call the API by using your browser or by using an HTTPS client to send a GET request.

For example:

```
curl -k --location -u <op_super_user>:<op_super_user_password>  
--header 'Content-Type: application/json' --header 'Accept: application/json'  
--cookie-jar cookie-jar.txt --cookie cookie-jar.txt --request GET 'https://  
<op_app_server>:<op_port>/grc/api/processes/<process_Id>'
```

In the response, the status attribute indicates whether the process is finished or still in progress. You can repeat the check as needed. The process is complete when the status value is `STATUS_FINISHED_SUCCESS`.

The encryption process can take time, depending on the data volume, especially if you have many file attachment records.

To check the logs for a process, you can send a GET request to the following endpoint:

```
https://<op_app_server>:<op_port>/grc/api/processes/<process_Id>/logs
```

Restarting the application servers

Restart the application server pods again.

Procedure

1. Scale down to 0 replicas.

```
oc scale --replicas=0 sts/openpages-<instance_name>-sts
```

To find the name of the StatefulSet (sts), run `oc get sts` and look for a name that starts with `openpages-`. For example, `openpages-instance_name-sts`

2. Wait until all application server pods are deleted.
3. Scale up to the number of replicas you want to use for the application server by running the following command:

```
oc scale --replicas=<#_of_replicas> sts/openpages-<instance_name>-sts
```

Replace the following values:

Variable	Replace with
<code><#_of_replicas></code>	Specify the number of replicas. Can be 1 or more.
<code><statefulset_name></code>	Specify the name of the StatefulSet for the application. To find the name of the StatefulSet, run <code>oc get sts</code> and look for a name that starts with <code>openpages-</code> .

Variable	Replace with
	For example, openpages-opinst-sts

Logging in to the database in IBM OpenPages for IBM Cloud Pak for Data

You can log in to the database from any application server pod. After you log in, you can run SQL commands by using CLPPlus.

Procedure

1. Log in to any of the application server pods.

Use one of the following methods:

Using the web client

In the Red Hat OpenShift console, go to an application server pod and open a terminal.

Using the command line

- a. Log in to your Red Hat OpenShift cluster as a project administrator:

```
oc login OpenShift_URL:port
```

- b. Change to the project where the IBM Cloud Pak for Data control plane is installed:

```
oc project <Project>
```

- c. Log in to the application server pod and open a terminal:

```
oc exec -it openpages-<instance_name>-sts-<N> -- /bin/bash
```

To find the pod name, run `oc get sts` and look for a name that starts with `openpages-`.

2. Log in to the database by running the following command:

```
clpplus -nw $OPDB_USER/$OPDB_PASSWORD@$OPDB_HOST:50000/OPX
```

The environment variables, such as `$OPDB_USER`, are already defined in the application server pod. You don't need to define them.

You are now logged in to the database and you can run SQL commands.

Updating IBM OpenPages Model Risk Governance for integration with OpenScale

If you want to use IBM OpenPages Model Risk Governance with IBM Watson OpenScale, do the following steps. This topic applies to IBM OpenPages for IBM Cloud Pak for Data.

Before you begin

- The ObjectManager tool is installed on a computer that has access to the cluster. See [“Installing tools and utilities \(IBM OpenPages with Watson\)”](#) on page 824.
- IBM Watson OpenScale is provisioned on IBM Cloud or Cloud Pak for Data.

Procedure

1. Locate the IBM OpenPages General package that you downloaded from Passport Advantage.
2. Locate the `8.2.0.x_MRG_Additional_Loader_Files.zip` file. Put the file in a new directory called `mrp-openscale`.

3. Expand the 8.2.0.x_MRG_Additional_Loader_Files.zip file.

You now have two loader files:

- Monitored_with_OpenScale_Filter-op-config.xml

This file contains a public filter for the Model object. The filter is called Models monitored with OpenScale. It enables users to filter on OpenScale models in grid views.

- OpenScale_Update_Metric_Last_Value_Info-op-config.xml

This file contains a workflow that updates Metrics that are associated with an OpenScale Model. The workflow updates Metrics with the most recent MetricValue values pushed from OpenScale.

4. Do steps 1-3 in “Preparing the instance” on page 46.

The instance is ready for a configuration change. One replica is running.

5. On the computer where the ObjectManager tool is installed, go to the openpages-tools-client/bin directory.

6. Run the following command to load the public filter.

Replace *<loader-file-path>* with the location of the Monitored_with_OpenScale_Filter-op-config.xml file.

```
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>  
<loader-file-path> Monitored_with_OpenScale_Filter
```

If you encounter any errors, review the log file, *<loader-file-path>/ObjectManager.log*.

7. Update the following profiles. If you use other profiles with MRG, update them also.

- **OpenPages Modules Master**
- **OpenPages MRG Master**
- **MRG Model Owner**
- **MRG Model Validation**

For information about working with profiles, see *IBM OpenPages with Watson Administrator's Guide*.

a) Log in to OpenPages as an administrator.

b) Click  > **Solution Configuration** > **Profiles**.

c) Click a profile.

d) For the **Model** object type, add the Models monitored with OpenScale filter.

e) For the **Metric** object type, add the following fields:

- Metric Type
- OpenScale Category
- OpenScale Description
- OpenScale Metric
- OpenScale Metric Value

f) For the **Metric Value** object type, add the following fields:

- Metric Type
- OpenScale Category
- OpenScale Description
- OpenScale Metric
- OpenScale Metric Value

8. Run the following command to load the workflow:

Replace `<loader-file-path>` with the location of the `OpenScale_Update_Metric_Last_Value_Info-op-config.xml` file.

```
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>  
<loader-file-path> OpenScale_Update_Metric_Last_Value_Info
```

If you encounter any errors, review the log file, `<loader-file-path>/ObjectManager.log`.

9. Do the steps in [“Backing up changes and implementing them across replicas”](#) on page 46.
10. Optional: Remove the `mrg-openscale` directory that you created in step 2.

Updating IBM OpenPages Financial Controls Management

IBM OpenPages for IBM Cloud Pak for Data 8.2.2 includes updates to IBM OpenPages Financial Controls Management (FCM). Do this task if you want to update FCM. This task is optional.

Before you begin

- The ObjectManager tool is installed on a computer that has access to the cluster. See [“Installing tools and utilities \(IBM OpenPages with Watson\)”](#) on page 824.
- OpenPages is provisioned on IBM Cloud or Cloud Pak for Data.

About this task

The new version of FCM includes the following components:

- New profiles, users, dashboards, and filters
- A new field group, OPSS-FCM-cert, and new fields
- New workflows for the following object types: Control, Control Eval, Process, Process Eval, Business Entity
- New system views for the following object types: Control, Control Eval, Process, Process Eval
- New calculations: Control Eval Certification and Process Eval Certification

Procedure

1. Download the IBM OpenPages Client Tools 8.2.0.2 Multiplatform Multilingual package from Passport Advantage.
2. Locate the `FCM_8202_Loader_Files.zip` file. Put the file in a new directory called `fcm-8202`.
3. Expand the `FCM_8202_Loader_Files.zip` file.
4. Do steps 1-3 in [“Preparing the instance”](#) on page 46.
The instance is ready for a configuration change. One replica is running.
5. On the computer where the ObjectManager tool is installed, go to the `openpages-tools-client/bin` directory.
6. Run the following command.

```
./Run_FCM_full.sh <op_admin_user> <op_admin_password>
```

If you encounter any errors, review the log file, `ObjectManager.log`.

7. Do the steps in [“Backing up changes and implementing them across replicas”](#) on page 46.
8. Optional: Remove the `fcm-8202` directory that you created in step 2.

Chapter 3. System Admin Mode (SAM)

Use System Admin Mode (SAM) to restrict user access to the system when you apply configuration changes or other updates to the system.

When System Admin Mode (SAM) is enabled, the following conditions are enforced:

- Only administrative users with **System Administration Mode** application permission can log on to the system. All other users are restricted from logging on.
- All Write operations are restricted, with these exceptions:
 - Reporting period operations if the reporting schema is not enabled
 - Metadata (schema) changes
 - Enumerated string conversions from single to multivalued selection
 - Setting changes that are made through the user interface

Before you enable SAM, you may want to notify application users to log off the system. If a user is already logged on to the system when SAM is enabled, the user will only be able to view objects and will not be able to create new instances of objects or save any modifications made to existing objects.

Depending on your configuration, SAM mode might not start until all asynchronous background jobs run to completion. For more information, see [“Asynchronous background jobs and administrative functions” on page 681](#).

You must be in System Admin Mode (SAM) if you:

- Want to create, re-create, enable, or drop a reporting schema. For more information see, [Chapter 6, “Managing the reporting schema,” on page 159](#).
- Have an existing reporting schema and you want to add, remove, or refresh a reporting period.
- Have configuration changes to make to the system, such as changes to the object model hierarchy or modifications to object types, field groups, and object fields.
- Are converting an enumerated string value from a single selection to a multi-value selection. For more information, see [“Defining enumerated string fields” on page 216](#).
- Set up field level security.

In all other instances you can make configuration changes without enabling SAM. However, there may be situations where you want to enable SAM to restrict general user access. For example, if you need to modify one or more object text labels, you may not want users to create new instances of the object type while you are making these changes.

Enabling and disabling System Admin Mode

You can enable and disable System Admin Mode (SAM).

About this task

If the system is processing operations that require System Admin Mode, you must wait until processing is complete before you can disable System Admin Mode.

Procedure

1. Log on to the IBM OpenPages with Watson user interface as a user with the **System Administration Mode** permissions.
2. To enable System Admin Mode, click  > **Enable System Admin Mode**.
3. To disable System Admin Mode, click  > **Disable System Admin Mode**.

Note: You can also enable or disable System Admin Mode in the Standard UI by using either of the following methods:

- Click the **Enable** or **Disable** link in the banner.
- Click **Administration** > **System Admin Mode** and click **Enable** or **Disable**.

Chapter 4. Users, groups, and domains

Access within the IBM OpenPages with Watson application is administered through the use of users, groups, and domains.

Users, groups, and domains can be managed using tasks in either the Task Focused UI or the Standard UI. Changes made in one interface are immediately reflected in the other.

To create and administer users and groups, you must have administrative privileges.

- To access the  > **Users and Security** > **Users** menu item in the Task Focused UI (or the **Administration** > **Users** menu item in Standard UI), you must have **Browse** permission on any security domain or any user group.
- To access the  > **Users and Security** > **Domains & Groups** menu item in the Task Focused UI (or the **Administration** > **Users, Groups and Domains** menu item in the Standard UI), you must be a Super Administrator or a delegated administrator with any administrator permission. For information about delegating and assigning administrator permissions, see [“Delegate administrator permissions” on page 76](#).
- For information about the administrative permissions that are required for specific user-provisioning functions, see [“Types of administrator permissions” on page 76](#).

Users and groups are organized under the following top-level groups:

- Security Domains

This group is a container for the security domain groups that are automatically created by the system when a business entity or sub-entity is added. You can use security domains to distribute your users and organizational groups so they can be administered by administrators with appropriate permissions. For an overview of security domains, see [“Security domains” on page 110](#).

When you expand a security domain group, only child security domains are displayed. Any organizational groups and users associated with that security domain can be viewed only from the detail page of that security domain group.

To view organizational groups and users associated with a security domain, navigate to the detail page of that security domain group.

- Workflow, Reporting and Others

This group is a container for organizational groups that are used system-wide. Administrators often create organizational groups to organize users and other groups. You can define all your users and groups under the Workflow, Reporting and Others group, and later associate them to different security domains. For upgrade customers, this top-level group also includes the groups that existed in prior releases of OpenPages with Watson.

To navigate to a group detail page, you must be a super administrator or a delegated administrator of that group with at least **Browse** administrative permission. For information on delegating administrator permissions, see [“Delegate administrator permissions” on page 76](#).

Note: The term group includes both organizational and security domain groups, unless otherwise specified.

Planning user administration

There are numerous things to consider before you create, modify, or copy a user account.

The following list outlines the tasks that you should perform before you begin creating, modifying, or copying users:

1. Determine whether you want to integrate IBM OpenPages with your LDAP servers to allow prepopulation of user information when you create a new user in IBM OpenPages. If so, then perform one or both of the following actions:
 - If you are using LDAP over SSL/TLS, [setup your certificates](#).
 - [Configure access to your LDAP servers from IBM OpenPages](#).
2. Determine whether you want to allow the creation or updating of users based upon existing users. The user will have the same attributes, such as locale, profiles, group memberships, role assignments, and reports access, as another user. If so, then perform the following actions:
 - [Determine which users can be used as source for the Copy Access From operation](#).
 - [Determine whether you want to allow inactive users to be the source for the Copy Access From operation](#).
 - [Configure the default behavior for the Locale, Profiles, Group Memberships, Direct Role Assignments, and Direct Reports Access attributes during the Copy Access From operation](#).
 - [Determine whether the Copy Access From operation adds to or replaces a user or group's existing attributes](#).
3. Determine the default values for the following settings:
 - [The default value or values for the Allowed Profiles](#).
 - [The default value for the locale](#).
 - [The number of rows that are listed per page in the Reports Access table](#).
4. Determine the password behavior for users by performing the following actions:
 - [Configure the default change password behavior when you create a new user](#).
 - [Configure the default password expiration behavior](#).
5. If user provisioning is configured in your system to allow copying attributes from inactive users, determine whether you want to create template users as inactive users. The inactive template users should have similar attributes that you want to copy to other users. The administrator can modify attributes after the copy operation.
6. Determine whether you want to add administrators who can perform user provisioning tasks beyond the super user. For example, you can create administrators who perform only password management tasks for users, while other administrators can create users.

Note: As of version 7.4, you must now assign delegated administrators rights at the top-level security domain and the top-level user group to perform some user-provisioning functions. For more information, see [“Administrator permissions for user-provisioning functions” on page 77](#). For these functions, you can separate out the tasks the delegated administrators can do but can no longer separate out which places they can perform them.

7. Determine whether you want to primarily manage administrative rights, such as managing profiles, role assignments, and reports access, directly at the user level or by making users members of user groups. You can use a combination of methods. It is strongly recommended that you manage administrator rights via user groups.
8. Determine the groups and security domains that you want each user to belong to. By default, when you create a new user from scratch, that user belongs to a special group called Standalone Users and Groups. Only the Super Administrator has administrative access to this group. When a user or group is disassociated from an organizational or security domain group, and that user or group is not a direct or indirect member of any other group, the system makes that user or group a member of Standalone Users and Groups.

For more information about group memberships, see [“Associating and disassociating a group \(Task Focused UI\)” on page 89](#).

9. Determine the profiles that you want the users to have.

For more information about choosing profiles, see [Chapter 11, “Profiles,” on page 297](#).

10. Determine the role assignments that you want the user to have.

For more information about role-based security and role templates, see [“Role-based security model” on page 105](#).

11. Determine the reports that you want the users to have access to.

For more information about modifying reports access, see [Chapter 7, “Managing reports,” on page 167](#).

12. If you use solutions, determine which sample users you want to keep.

For each sample user that you want to keep, reset the user's password. See [“Modifying user accounts” on page 86](#).

Disable the sample users that you don't need.

The Super Administrator

A Super Administrator is a user who has complete access to all objects, folders, role templates, and groups in the system. A deployment can have one or more Super Administrators.

- A Super Administrator can create users, groups, and other super administrators.
- A Super Administrator can delegate administration activities by assigning roles to users through the use of role templates (for more information see [“Role templates” on page 113](#)) and group administrator permissions (for more information, see [“Delegate administrator permissions” on page 76](#)).

For example, a Super Administrator can delegate user provisioning functions to other administrators. For more information, see [“Administrator permissions for user-provisioning functions” on page 77](#).

A Super Administrator is specified during the installation process. In a new installation, the Super Administrator is the only user in the system. In an upgrade, you can enter a new user or select one of the existing users (such as SOXAdministrator or OpenPagesAdministrator) as a Super Administrator.

Creating a Super Administrator

If you are logged in to IBM OpenPages with Watson as a Super Administrator, you can create other super administrators.

You create a Super Administrator by adding Super Administrator status to an existing user account.

1. Click  > **Users and Security** > **Users** and select the user account that you want to modify.

Or, in the Standard UI, click **Administration** > **Users**.

For more information, see [“Modifying user accounts” on page 86](#).

2. On the **User Information** page, set **Super Administrator** to true. In the Standard UI, **Super Administrator** is a check box.

The field is grayed-out if:

- You are not logged in as a Super Administrator.
- You are modifying your own user account.

Tip: You can delegate administrator activities instead of (or in addition to) creating Super Administrators. See [“Role templates” on page 113](#) and [“Delegate administrator permissions” on page 76](#)

You can revoke Super Administrator status by setting **Super Administrator** to false. The field is grayed-out if:

- You are not logged in as a Super Administrator.
- You are modifying your own user account.
- Only one Super Administrator is configured. Each deployment must have at least one Super Administrator.

Delegate administrator permissions

By assigning specific security management permissions to an administrator's user account, you can delegate various security management activities to that administrator. For example, you could set up one administrator who would only have the ability to reset passwords for users, another who could lock and unlock users, and a third who could create users and associate them to user groups and assign them role templates.

For more information about entity groups, see “Security context points” on page 107). If there are child groups under a parent group, the administrator can delegate an administrator for each child group as well.

Administrators do not have to be members of groups for which they perform administrative tasks. By default, only the Super Administrator has Read and Write access to objects in the system. Delegating administration responsibilities to a user on a security domain, does not automatically grant Read and Write access to objects under the corresponding entity.

Important:

- You can only assign those permissions that you have to other administrators.
- If you disassociate an administrator from a security domain or organizational group, all user management privileges (such as manage users, lock/unlock users, reset passwords, enable/disable users, assign roles) are retained by that administrator and are not revoked.

Example

You want to designate Mary Smith as an administrator who can reset passwords for any users. You would assign the **Reset Password** permission to Mary Smith.

Note:

- When administrator permissions are assigned to a user, the name of that user is no longer displayed in the user selector list. To modify permissions for an administrator, see “Assigning, modifying, and removing administrator permissions on groups (Task Focused UI)” on page 79.
- Security domain groups are not displayed in the User/Group selector list.

Note: Administrators with **Settings** application permission can configure the behavior of some user-provisioning functions. For more information, see “User provisioning settings” on page 603.

Types of administrator permissions

There are six security management permissions that you can delegate to a security domain or user group administrator.

Table 49. Administrator permissions	
Permission	Description
Manage	Allows the delegated administrator to create, modify, and associate users and groups.
Lock	Allows the delegated administrator to lock a user account, which prevents logon to the IBM OpenPages with Watson application from that account. With this permission, a Lock User link can be clicked in the User Information section of a user account.
Unlock	Allows the delegated administrator to unlock a previously locked user account. With this permission, an Unlock User link can be clicked in the User Information section of a user account.
Reset Password	Allows the delegated administrator to reset passwords for users.

Table 49. Administrator permissions (continued)	
Permission	Description
Assign Role	Allows the delegated administrator to assign one or more roles to users and groups and to revoke a role from a user or group. This permission applies to security domains only.
Browse	Allows the delegated administrator to view users and groups within that group. This permission is selected by default.

Administrator permissions for user-provisioning functions

You must have the appropriate administrator permissions to perform each user-provisioning function.

Table 50. Permissions required for user provisioning functions	
To do the following...	You must have these permissions...
View: - The  > Users and Security > Users menu item (Task Focused UI) - The Administration > Users menu item and the View, Edit, or Disable User field on the Users landing page (Standard UI)	Browse on any security domain or any user group.
View: - The Create User button from a list of users and create new users (Task Focused UI) - The Create User button on the Users landing page and create new users (Standard UI)	Manage on any security domain or any user group. If LDAP Server integration is configured, there is an additional field that you can use to search for user in LDAP Server and prepopulate their user information. For more information, see “LDAP and user provisioning” on page 81.
Edit user information	Manage on any security domain or any user group that includes the user account.
Enable and disable user accounts	Manage on any security domain or any user group that includes the user account. To clear direct role assignments when you disable a user account, you must have Assign Role on the root security domain. To clear group memberships when you disable a user account, you must have Manage on the top-level user group. To clear direct reports access when you disable a user account, you must belong to the OPA administrators group. Note that an administrator cannot disable their own account. For information about the difference between disabling and locking user accounts, see “Modifying user accounts” on page 86.

Table 50. Permissions required for user provisioning functions (continued)

To do the following...	You must have these permissions...
Lock user accounts	Lock on any security domain or any user group that includes the user account. Note that an administrator cannot lock their own account.
Unlock user accounts	Unlock on any security domain or any user group that includes the user account.
Edit user passwords This includes the Password and Confirm Password fields.	Reset Password on any security domain or any user group that includes the user account.
Configure password options and edit configured password options This includes the following options: User must change password at next log on , User cannot change password , Password never expires , Password expires in <n> days , and Force Password Change .	Manage on any security domain or any user group that includes the user account. Note that an administrator can force a password change for their account and reset their password.
Edit a user's locale and profile information	Manage on any security domain or any user group that includes the user account.
Modify a user's group memberships	Manage on the top-level user group.
Add role assignments to a user	Manage and Assign Role on the root security domain.
Remove role assignments from a user	Assign Role on the root security domain.
View a user's reports access	OPAdministrators group membership. Information is read-only.
Copy access from one user to a new or existing user This includes locale, profiles, group memberships, and direct role assignments.	Manage on the top-level user group and Manage and Assign Role on the root security domain.
Copy direct reports access from one user to a new or existing user	Manage on the top-level user group, Manage and Assign Role on the root security domain, and OPAdministrators group membership. Information is read-only.

Example

Figure 3 on page 79 shows a diagram with a sample security administration structure.

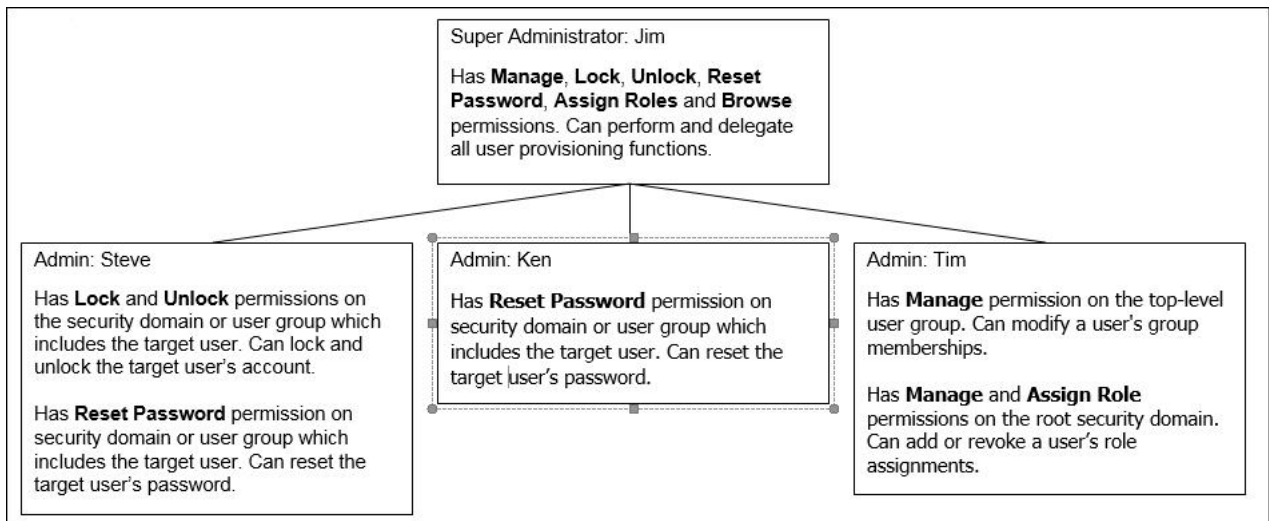


Figure 3. Sample security administration

Assigning, modifying, and removing administrator permissions on groups (Task Focused UI)

You can assign one or more group administrator permissions to selected users. You can also modify and remove group administrator permissions.

About this task

A group contains the following sections:

- **Group Information**
- **Administrators & Permissions**
- **Groups**
- **Users**
- **Role Assignments**
- **Permissions**

Procedure

1. Click  > **Users and Security** > **Domains & Groups**.
2. Click **Groups**.
3. Expand the folder structure to find the group you want to work with.
4. Click the name of the group for which you want to assign administrative permissions to selected users.
The detail page of the selected group is displayed.
5. To assign administrator permissions, go to the **Administrators & Permissions** section.
 - a) Click **Add**.
 - b) Search for and select a user or group.
 - c) From the **Permissions** column, select the administrative permissions that you want to assign to this user (see [“Types of administrator permissions”](#) on page 76 for a list of permissions).
 - d) Click **Add**.
6. To remove a user or group's administrator permissions entirely, go to the **Administrators & Permissions** section.
 - a) From the list of administrative users, click the check box next to the user or group.

- b) Click **Remove**.

Assigning administrator permissions (Standard UI)

You can assign one or more group administrator permissions to selected users.

Procedure

1. Click **Administration > Users, Groups and Domains**.
2. On the **Users, Groups and Domains** page, click the name of the group for which you want to assign administrative permissions to selected users.
3. On the detail page of the selected group, go to the **Administrators & Permissions** tab.
4. Click **Assign**.
5. Select (user icon ) or search for a user (magnifying glass icon )
6. From the **Permissions** column, select the administrative permissions that you want to assign to this user (see [“Types of administrator permissions”](#) on page 76 for a list of permissions). To select all permissions, select the **Permissions** box in the column heading.
7. When finished, click one of the following icons:
 - **Assign** to return to the selected group's detail page.
 - **Assign & Next** to assign administrative permissions to another user.

Modifying administrator permissions (Standard UI)

You can modify administrator permissions that are assigned to a user at any time.

Procedure

1. Click **Administration > Users, Groups and Domains**.
2. On the **Users, Groups and Domains** page, click the name of the group for which you want to modify administrative permissions.
3. On the detail page of the selected group, go to the **Administrators & Permissions** tab.
4. From the list of administrative users, click the pencil icon  next to the user whose permissions you want to edit.
5. In the **Specify Permissions** box, select or clear administrative permissions for this user (see [“Types of administrator permissions”](#) on page 76 for a list of permissions).
6. Click **Save**.

Revoking administrator permissions (Standard UI)

You can revoke administrator permissions that are assigned to one or more users.

Procedure

1. Click **Administration > Users, Groups and Domains**.
2. Click the appropriate group, and on the **Users, Groups and Domains** page, select the check box next to the name of each user in the **Administrators** list for whom you want to revoke administrative permissions.
3. Click **Revoke**. The name of the user is removed from the list of group administrators.

LDAP and user provisioning

You can configure access to your LDAP server or servers from IBM OpenPages with Watson so that you can access user information from your LDAP server or servers when creating users in IBM OpenPages.

Through an LDAP server integration with IBM OpenPages, you can search your company's LDAP servers for a list of people who meet the search criteria. You can then select a user from the list and the information fields in the **Create User** page will be pre-populated with the user's information from the LDAP server.

Note: LDAP configuration for user provisioning does not affect LDAP user authentication.

Importing an LDAP certificate to the local trust store

If you are using LDAP over SSL/TLS, you must import an LDAP certificate to the local trust store before you can configure LDAP for user provisioning. It is needed to build a secure communication between the OpenPages with Watson servers and your LDAP over SSL/TLS server.

Before you begin

The target LDAP server from which you are going to retrieve the certificate must be running and listening on the port.

Procedure

1. Get the certificate from your LDAP server by using your browser or openssl.
2. Import the certificate by running this command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_NAME> -keystore  
<STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- <CERTIFICATE_ALIAS> type an alias for the certificate.
- <CERTIFICATE_NAME> is the file name of the certificate.
- <STORE_PATH> is the full path and file name of the trust store on the application server. For example: <OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security/key.p12
- <STORE_PASSWORD> is the password of the trust store on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

3. Restart the OpenPages with Watson application services.
4. Repeat these steps on each application server.

Configuring LDAP access for user provisioning (Task Focused UI)

You can configure access to your LDAP server to import LDAP user information when you create users in IBM OpenPages with Watson.

Before you begin

To configure LDAP access for user provisioning, you must be a member of the OPAdministrators user group and have the following application permission; **All Permissions > SOX > Administration > LDAP Server**.

If you are using LDAP over SSL/TLS, complete the [preconfiguration task](#) first.

Procedure

1. Click  > **Users and Security** > **User LDAP Configuration**.
2. Click **Add New**.
3. Type a name for the LDAP configuration.

You can configure multiple LDAP servers. When you use multiple servers, the **Create User** page shows the search results from all LDAP servers. The maximum number of search results displayed on the page is the sum total of the maximum results configured for each LDAP server.

4. In the **Provider URL** field, type the LDAP service provider that you want to use.

The value must be a URL string, such as `ldap://<hostname>:389`.

Or, if you are using SSL/TLS: `ldaps://<hostname>:636`

Note: If you are using LDAP over SSL/TLS, you need to do some additional [preconfiguration](#) steps.

5. Enter the values for your LDAP server. For information about a field, click the field.

Required fields have a red * next to the field name.

In the **First name attribute**, **Middle name attribute**, and **Last name attribute** fields, type the attribute names that you want to map to the OpenPages user's given name, middle name, and surname.

Note: The middle name is not displayed in OpenPages by default. You might want to display it so that you can differentiate users who have the same given name and surname. To display the middle name in the search results of the **Create User** page, add the following code to **Application Text** > **Formats** > **com.display.name.format**: %MN. For more information, see [“Modifying the user name format”](#) on page 568. The middle name is not stored in OpenPages.

6. Click **Validate**.

If a required field is missing or contains an incorrect value, a message is displayed.

7. After you successfully validate the information, click **Save**.

Configuring LDAP access for user provisioning (Standard UI)

You can configure access to your LDAP server to import LDAP user information when creating users in IBM OpenPages with Watson.

Before you begin

To configure LDAP access for user provisioning, you must be a member of the OPAdministrators user group and have the following application permission; **All Permissions** > **SOX** > **Administration** > **LDAP Server**.

If you are using LDAP over SSL/TLS, make sure you have completed the [preconfiguration task](#).

Procedure

1. Click **Administration** > **User LDAP Configuration**.
2. Click **Add New**.
3. Type a name for the LDAP configuration and click **OK**.

Note: You can configure multiple LDAP servers so that the **Create User** wizard shows the search results from all LDAP servers at once. The maximum number of search results, is the sum total of the maximum results of each LDAP server configured.

4. In the **Provider URL** field, type the LDAP service provider that you want to use.

The value should contain a URL string, such as `ldap://<hostname>:389`.

Note: If you are using LDAP over SSL/TLS, there are some additional [preconfiguration](#) steps that you must perform. An example for the **Provider URL** when using LDAP over SSL/TLS is the following string: `ldaps://<hostname>:636`.

5. Enter the values for your LDAP server. For information about a field, click .
6. In the **First name attribute** field, **Middle name attribute** field, and **Last name attribute** field, type the attribute names that you want to map to the IBM OpenPages user's first name, middle name, and last name respectively.
Note: The middle name is not displayed in IBM OpenPages by default. To display the middle name in the search results of the **Create User** wizard so that you can differentiate users who have the same first and last name, you can add the following code to the **Label** box of the **com.display.name.format** entry under the **Formats** folder on the **Application Text** page: %MN. For more information, see [“Modifying the user name format” on page 568](#). The middle name is not stored in IBM OpenPages.
7. Click **Validate** to ensure you have filled out the form correctly.
If you have missed a required field or entered incorrect information, an error message is displayed at the top of the screen.
8. After you have successfully validated the information, click **Save**.

Provisioning users

Your ability to create a new user, modify user accounts, and copy access from one user to another is based on your administrative permissions and the way user provisioning is configured in your system. The user-provisioning options that you see in the product are determined by your permissions and configuration.

You can delegate administrative capabilities to specific administrators to give them the ability to perform certain user-provisioning functions. For example, you could delegate permission to two administrators to manage user passwords, and delegate permission to three other administrators to create users and update group memberships.

For information about which administrator permissions are required for each of the user-provisioning functions, see [Table 50 on page 77](#).

Creating user accounts (Task Focused UI)

You create new user accounts on the **Create User** page.

Before you begin

Before you create a new user, see [“Planning user administration” on page 73](#).

About this task

Depending on your permissions and user provisioning configuration, you can copy access from an existing user to a new one. You can also copy access from one existing user to another. For more information, see [“Modifying user accounts” on page 86](#).

Depending on your delegated administrator permissions, you can perform certain functions when you create a user account, such as associating group memberships and assigning roles. For information about which permissions you need for each operation, see [“Administrator permissions for user-provisioning functions” on page 77](#).

Procedure

1. Click  > **Users and Security** > **Users**.
2. Click **Create User**.

Note: If you see a **Copy users from LDAP server** button, you can import user information from your organization's LDAP server. Click **Copy users from LDAP server** to search for and select a user. For information about configuring access to an LDAP server, see [“Configuring LDAP access for user provisioning \(Task Focused UI\)” on page 81](#).

3. Complete the information in **User Information** and **Password and Security**.

When you create user names and passwords, the following rules apply:

- User names are case-sensitive. For example, MyName and myname would be two unique users.
- User names can be up to 256 characters.
- User names can contain alphanumeric characters and any of the following special characters:
@ - ! . _ / : * \ " # % ? < >

To exclude characters, including special characters, from user names, specify these characters in the **Illegal Characters** setting. For more information, see [“Exclude characters from user names” on page 635](#).

- Passwords can contain up to 32 characters and cannot contain spaces.

If LDAP authentication is configured for your OpenPages application, you can specify how a user is authenticated when the user logs in to OpenPages. Click **Authenticate from**.

- If you want the user to authenticate by using OpenPages, select **Native**.
- If you want the user to authenticate by using an LDAP server, select the LDAP server from the list. If you do not see any LDAP servers in the list, no LDAP servers are configured for user authentication.

4. In the **Locale and Profiles** section, you can specify the user's locale, choose one or more profiles to associate with the user, and select a **Current Profile**.
5. If you have the necessary permissions, you can copy access from another user to determine the starting point for a new user's attributes, such as group memberships, role assignments, and reports access.

In **Copy Access From**, click **Select user to copy from**. Type a user name, first name, last name, or email address. Select a user, and then click **Copy**. When you click **Save**, the new user is updated with the access settings of the source user. Personal filters are not copied.

6. Click **Save**.
7. In the **Group Memberships** section, perform the following actions to assign group memberships:
- To select group memberships, click **Associate Groups** and select the check boxes next to the groups to which you want the user to be a member.
 - To delete group memberships, click  next to the membership that you want to remove.
8. In the **Role Assignments** section, you can view the user's role assignments. To add role assignments, click **Assign Roles**.
9. In the **Reports Access** section, you can view the user's reports access.
10. Click **Save**.

Creating user accounts (Standard UI)

You create new user accounts with the **Create User** wizard.

Before you begin

Before you create a new user, see [“Planning user administration” on page 73](#).

Tip: You can create and modify users in the Task Focused UI.

About this task

Depending on your permissions and user provisioning configuration, you can copy access from an existing user to a new one. You can also copy access from one existing user to another. For more information, see [“Modifying user accounts” on page 86](#).

Depending on your delegated administrator permissions, you can perform certain functions when you create a user account, such as associating group memberships and assigning roles. For information about

which permissions you need for each operation, see [“Administrator permissions for user-provisioning functions”](#) on page 77.

Procedure

1. Click **Administration > Users**.
2. Click **Create User**.

Note: If LDAP is configured with your IBM OpenPages with Watson application, a **Search** field is displayed. This allows you to search for an LDAP user whose information you want to copy to create the new IBM OpenPages user. You can type a user name, first name, last name, or email address into the **Search** field. Select the LDAP user from the list to access the **Create User** page. For information about configuring access to an LDAP server, see [“Configuring LDAP access for user provisioning \(Standard UI\)”](#) on page 82.

3. Complete the information on the **User Information** and **Password and Security** pages of the **Create User** wizard.

When you create user names and passwords, the following rules apply:

- User names are case-sensitive. For example, MyName and myname would be two unique users.
- User names can be up to 256 characters.
- User names can contain alphanumeric characters and any of the following special characters:
@ - ! . _ / : * \ " # % ? < >

To exclude characters, including special characters, from user names, specify these characters in the **Illegal Characters** setting. For more information, see [“Exclude characters from user names”](#) on page 635.

- Passwords can contain up to 32 characters and cannot contain spaces.

If LDAP authentication is configured for your IBM OpenPages with Watson application, you can specify how a user is authenticated when the user logs in to OpenPages. Click **Authenticate from**.

- If you want the user to authenticate by using OpenPages, select **Native**.
 - If you want the user to authenticate by using an LDAP server, select the LDAP server from the list. If you do not see any LDAP servers in the list, no LDAP servers are configured for user authentication.
4. If you have the necessary permissions, you can copy access from another user to determine the starting point for a new user's attributes, such as group memberships, role assignments, and reports access. On the **Copy Access From** page, perform one of the following actions:
 - Click **Assign from scratch**, and then click **Next**.
 - Click **Select user to copy from**.
 - Search for the user that you want to use as source for the copy operation. You can type a user name, first name, last name, or email address to find a user.
 - Click **Next**. The following pages of the **Create User** wizard reflect the locale, profiles, group memberships, role assignments, and reports access of the source user. Personal filters are not copied.

5. On the **Locale and Profile** page, you can specify the user's locale, choose one or more profiles to associate with the user, and select a **Current Profile**.
6. On the **Group Memberships** page, perform the following actions to assign group memberships:
 - To select group memberships, click **Associate Groups** and select the check boxes next to the groups to which you want the user to be a member.
 - To delete group memberships, click the **X** next to the membership that you want to remove.
7. On the **Role Assignments** page, you can view the user's role assignments.
You can assign roles after the user is created.
8. On the **Reports Access** page, you can view the user's reports access.
9. Click **Finish**.

Modifying user accounts

You can view and modify the details of an existing user account, such as all the user's group memberships, role assignments, and profiles.

Before you begin

Before you modify user information, see [“Planning user administration” on page 73](#).

About this task

Depending on how user provisioning was configured in your system, you might be able to copy access from one user to another. For information about copying access, see [“Copying access from one user to another” on page 87](#).

Depending on your delegated administrator permissions, you can perform certain functions when you modify a user account, such as editing user information, enabling or disabling a user account, and changing group memberships. For information about which permissions you need for each editing operation, see [“Administrator permissions for user-provisioning functions” on page 77](#).

There are some constraints on your ability to make changes. For example, you cannot disable or lock yourself, the default Super Administrator (OpenPagesAdministrator), or the OPSysSystem user. You cannot remove a user from special user groups that contain all users, or all users who are not associated with any other user group.

If you are logged in as a Super Administrator, you can add or remove super administrator status from other user accounts. For more information, see [“Creating a Super Administrator” on page 75](#).

Procedure

1. Click  > **Users and Security** > **Users**.

Or, in the Standard UI, click **Administration** > **Users**.

2. Search for the user account that you want to modify.

3. In the **User Information** section, you can perform one or more of the following actions:

- Edit user details, such as email, first name, and last name. You cannot change a user name.
- Disable and enable a user account. When an account is disabled, the user of that account is prevented from logging in, and the user is displayed as inactive and grayed out in user selector lists. If necessary, you can re-enable a disabled user account. User accounts cannot be deleted through the user interface in IBM OpenPages. Depending on how your system is configured, in addition to disabling the user, you can choose to remove their locale, profile, group membership, role assignment, or reports access.

Tip: If you want to prevent a user from logging in, but you still want the user to appear in user selectors, disable the user and then update the user selectors to set **Include Disabled** to **True**. For more information, see [“Defining user/group fields” on page 219 \(Task Focused UI\)](#) or [“Configure user and group selectors display types for simple strings \(Standard UI\)” on page 353 \(Standard UI\)](#).

- Lock and unlock a user account. Depending on your configuration, users might be locked automatically if they exceed a set number of unsuccessful login attempts. When an account is locked, the user of that account is prevented from logging in. The user is displayed as active but locked in user selector lists, and they can be selected. If you do not want the user to appear as active and selectable in user selector lists, disable the user account instead.
- Reset the user's password or force the user to change the password the next time they log on. Passwords can contain up to 32 characters and cannot contain spaces.

Important: If you use IBM OpenPages Loss Event Entry, do not modify the dedicated users' passwords by using OpenPages. Always use the Loss Event Entry Configuration tool. Also, the **User cannot change password** and **Password never expires** options must be selected for the dedicated user accounts.

If LDAP authentication is configured, you can also change the authentication method for the user. Click **Reset Password**, and then click the **Authenticate from** list.

4. In the **Locale and Profile** section, you can change the user's locale, change the **Allowed Profiles**, and select a different **Current Profile**.
5. In the **Group Memberships** section, you can add and remove group membership assignments by clicking **Associate Groups**.
6. In the **Role Assignments** section, you can add role assignments by clicking **Assign Roles**.

You can remove role assignments that were assigned directly to the user. You cannot remove role assignments that are inherited from group memberships.

When you remove a role from a user or group, the role assignment is explicitly removed from the user or group on a given entity. The user is not, however, disassociated from the security domain.

7. In the **Reports Access** section, you can view the reports folder access that was assigned directly to the user and inherited from group memberships.

What to do next

If you removed a role assignment from a user or group, disassociate the user from the security domain.

Copying access from one user to another

You can copy a user's locale, profiles, group memberships, and direct role assignments. You can also copy direct reports access attributes to another user.

Before you begin

Before you copy access from one user to another, see [“Planning user administration”](#) on page 73.

To copy access from one user to another, you must be granted **Manage** permission at the top-level group and **Assign Role** and **Manage** permissions at the root security domain. If you do not have these permissions, you cannot see the **Copy Access From** option.

Administrators with **Settings** application permission can use the user provisioning registry settings to establish the following copy access behavior:

- Determine whether the copy operation is allowed and which users, including inactive users, can be used as sources for the copy operation. For more information, see [“Users Can Copy Access From”](#) on page 605 and [“Copy Access From Inactive”](#) on page 603.
- Specify which attributes are copied by the copy operation. For more information, see [“Copy User Info Attributes”](#) on page 604.
- Determine whether the copy operation adds to or replaces the user's existing attributes. For more information, see [“Copy User Info Choice”](#) on page 604.

Procedure

1. Click  > **Users and Security** > **Users**.

Or, in the Standard UI, click **Administration** > **Users**.

2. Search for the user account that you want to modify.

Note: You can also copy access from an existing user when you are creating a new user. For more information, see [“Creating user accounts \(Task Focused UI\)”](#) on page 83. If you are using the Standard UI, see [“Creating user accounts \(Standard UI\)”](#) on page 84.

3. From the left pane, click **Copy Access From**.
4. Search for the user that you want to use as the source.
5. Click **Copy**.

Note: Personal filters are not copied.

Creating an organizational group (Task Focused UI)

Users with the correct permissions can create groups. Groups can contain other groups and users, and inherit application permissions from the groups that they belong to.

Procedure

1. Click  > **Users and Security** > **Domains & Groups**.
2. Click **Groups**.
3. Expand the list and click the name of the group to which the new group belongs. If no higher-level group for the new group exists, select the **Workflow, Reporting and Others** group.
4. From the selected group page, go to the **Groups** section and click **New**.
5. Complete the required information for the new group and click **Add**. The parent group's page is displayed with the new group listed in the **Groups** section.
6. Open the group from the **Groups** tab and complete the remaining sections:
 - **Administrators & Permissions**
 - **Groups**
 - **Users**
 - **Role Assignments**
 - **Permissions**

Associating and disassociating a group (Task Focused UI)

You can associate and disassociate groups from other groups.

When you disassociate a group and that group does not belong to any other IBM OpenPages with Watson group, the group is listed under the special group that is named **Standalone Users and Groups**, which is under the top-level **Workflow, Reporting and Others** group. You cannot add and remove groups directly from the **Standalone Users and Groups** group.

When you add an existing group to another group, the disassociated group is still available in the group selector list.

Procedure

1. Click  > **Users and Security** > **Domains & Groups**.
2. Click the **Groups** tab.
3. Expand the list and click the name of the group to which you want to associate another group, or to which the soon-to-be-disassociated group belongs.
4. Go to the **Groups** section.
5. Click **New** to create a group and associate it to the selected group. For more information, see [“Creating an organizational group \(Task Focused UI\)”](#) on page 88.
6. Click **Add** to add an existing group to the selected group.
7. Click **Remove** to remove a group.

Creating an organizational group (Standard UI)

Users with the correct permissions can create groups by using the User/Group interface. Groups can contain other groups and users, and inherit application permissions from the groups that they belong to.

Procedure

1. Click **Administration** > **Users, Groups and Domains**.
2. Expand the list and click the name of the group to which the new group belongs. If no higher-level group for the new group exists, select the **Workflow, Reporting and Others** group.
3. On the detail page of the selected group, go to the **Groups** tab and click **Add New**.
4. Complete the required information for the new group and click **Create**. The parent group's detail page is displayed with the new group listed in the **Groups** section.
5. If you want to add users to the group or modify the group permissions, click the name of the new group to view the detail page.

Associating and disassociating a group (Standard UI)

You can associate and disassociate groups from other groups.

When you disassociate a group and that group does not belong to any other IBM OpenPages with Watson group, the group is listed under the special group that is named **Standalone Users and Groups**, which is under the top-level **Workflow, Reporting and Others** group.

When you add an existing group to another group, the disassociated group is still available in the group selector list.

Procedure

1. Click **Administration** > **Users, Groups and Domains**.
2. Expand the list and click the name of the group to which you want to associate another group, or to which the soon-to-be-disassociated group belongs.

3. Go to the **Groups** tab and select the check box next to each group to be associated or disassociated.
4. Click **Associate** or **Disassociate**.

Defining application permissions

You can define access permissions for IBM OpenPages with Watson.

The following methods of defining permissions are available:

- In **Role Templates** - this is the preferred method for granting users or groups application permissions.

Note:

- Both application permissions and ACLs are included in the role definition process. When a role is assigned to a user or a group on any business entity or security context point, that user or group automatically acquires the application permissions defined in that role template.
- When a user or group is assigned multiple roles, the user or group accumulates the application permissions that are defined in the various roles. Application permissions are granted by the role (not the security context point) and apply in all situations where the user has the correct ACL access. For example, users with Read permission to Business Entities and the **Audit Trail** application permission will be able to view the Change History (audit trail) for those Business Entities.

For more information, see [“Role templates” on page 113](#).

- As part of an organizational group definition - this method is provided for backward compatibility for upgrade customers and for administering system-wide organizational groups. Organizational groups can be created under the **Workflow, Reporting and Others** root folder on the **Users, Groups and Domains** page. For more information, see [“Creating an organizational group \(Task Focused UI\)” on page 88](#).

Setting group application permissions

By setting application permissions on a group (either through a role template or on organizational groups), you can control, for example, whether users in that group can lock objects, view audit trail information, and create reporting periods.

To delegate group security management permissions to administrators, see [“Delegate administrator permissions” on page 76](#).

To assign application permissions for a role, see [“Accessing Role Templates” on page 113](#).

Procedure

1. Click  > **Users and Security** > **Groups & Domains**.

Or, in the Standard UI, click **Administration** > **Users, Groups and Domains**.

2. Click **Groups**.
3. Expand the list and click the name of the group whose application permissions you want to view or modify.
4. On the selected group, go to the **Permissions** section.

Tip: Most of the application permissions in IBM OpenPages with Watson are grouped under the SOX heading. Selecting the SOX permission selects all the permissions under that heading. This is only advisable for administrative level users.

For a description of the various permissions, see [“Types of application permissions” on page 91](#) and [“Application permissions not contained under the SOX heading” on page 97](#).

5. To modify application permissions for a group, click **Edit**, make the required changes, and then click **Done**.
6. To assign user and group management permissions to selected users, see [“Delegate administrator permissions” on page 76](#).

Types of application permissions

Administrators can use a set of application permissions to limit the activities of the various users and user groups that can access the IBM OpenPages with Watson application. The application permissions reside under the SOX permissions heading and can be applied to OpenPages with Watson user groups.

Important: If the changes to application permissions result in changes to menus, the menu changes do not appear until users log out and then log back in to the application.

Users are generally granted applicable permissions by being assigned to role templates that include those permissions.

Administration permissions

When you create an administrative-level group, you must grant them Administration permissions.

In the Standard UI, if a user or user group possesses any of the Administration permissions, they see the **Administration** menu on the menu bar.

Table 51. Administration application permissions

Permission	Description
Access Control Lists	Allows super administrators to view, edit, and remove the access control listings for objects. For more information, see “Role-based access control permissions” on page 111.
Application Text	Allows users and members of user groups to view and edit locale-specific application label values. For more information, see “Localizing application text” on page 564.
Ascent Feed	Allows users and members of user groups to configure the import of Ascent Reg Tech data by using the Ascent job in the Scheduler.
Bulk Update All Fields	Allows administrators to use the Bulk Update feature on all fields in grid views. For more information, see “Designing a Grid View” on page 374.
Calculation	Allows users and members of user groups to create, delete, and modify calculation definitions through the  > Solution Configuration > Calculations menu item in the Task Focused UI. For more information, see Chapter 14, “Configuring GRC Calculations,” on page 457.
Cognitive	Allows administrators to configure natural language classifiers. For more information, see “Natural language processing services ” on page 1021.
CompareEnvironments	Allows users and members of user groups to use the Compare Environments tool through the Administration > Compare Environments menu item in the Standard UI. For more information, see Chapter 25, “Comparing IBM OpenPages with Watson environments,” on page 853.
Currencies	Allows users and members of user groups to administer currencies. For more information, see “Modifying currency exchange rates” on page 213.

Table 51. Administration application permissions (continued)

Permission	Description
Dashboards	Allows administrators to create and manage dashboards through the  > Solution Configuration > Dashboards menu item in the Task Focused UI. For more information, see “Home page, dashboard, and tabs in the Task Focused UI” on page 367
Encryption Keystore	Allows administrators to configure the encryption keystore through the  > Users and Security > Encryption Keystore menu item in the Task Focused UI. For more information, see “Encryption” on page 146.
ExportConfiguration	Allows users to access the environment migration tool to export configuration items for import into another system. Read and write access to the Migration Documents folder is also required. For more information, see Chapter 26, “Migrating OpenPages environments,” on page 865.
FastMap	Allows a user to import object data and to view imports performed by other users. Import allows users to import object data and to see their import history using the FastMap Import menu item in the Task Focused UI. View all history allows users to view imports performed by other users in the Task Focused UI. When a user has this permission, the Created By column is added to the grid on the FastMap Import tab. For more information, see Chapter 28, “Using FastMap ,” on page 915.
Field Groups	Allows users and members of user groups to view and manage the configuration of field groups through the  > Solution Configuration > Objects menu item and the Field Groups section in the Task Focused UI and the Administration > Field Groups menu item in the Standard UI.
ImportConfiguration	Allows users to access the environment migration tool to import configuration items that are exported from another system. Read and write access to the Migration Documents folder is also required. For more information, see Chapter 26, “Migrating OpenPages environments,” on page 865.
LDAP Server	Allows Super Administrators to configure the LDAP server for user provisioning. For more information, see “LDAP and user provisioning” on page 81.
Notification Manager	Allows Super Administrators and users to run the Notification Manager tool. For more information, see Appendix A, “The Notification Manager,” on page 1075.
NPS	Allows users and members of user groups to configure the Net Promoter Score (NPS) with the  > Integrations > NPS Settings menu item in the Task Focused UI.

Table 51. Administration application permissions (continued)

Permission	Description
Object Profiles	Allows users and members of user groups to view and manage profiles, which include object types, through the  > Solution Configuration > Profiles menu item in the Task Focused UI and the Administration > Profiles menu item in the Standard UI.
Object Reset	Allows users and members of user groups to reset objects for a new reporting period. For information on governing reset behavior, see Chapter 18, “Reporting periods, object resets, and rulesets,” on page 577.
Object Text	Allows users and members of user groups to view and edit locale-specific object label values. For more information, see “Localizing object text” on page 561
Object Types	Allows users and members of user groups to view and manage object types through the  > Solution Configuration > Objects menu item in the Task Focused UI. Allows users and members of user groups to view and manage solution schema visualizations, through the  > Solution Configuration > Solutions menu item in the Task Focused UI. Allows users and members of user groups to view and manage object types, along with their related field groups and associated objects, through the Administration > Object Types menu item in the Standard UI.
RegTrack Feed	Allows users and members of user groups to configure the import of Reg-Track data through the  icon on the Regulatory Compliance > Reg-Track Regulatory Events page in the Task Focused UI.
Reporting Framework	Allows users and members of user groups to generate and manage the reporting framework. For more information, see “Generating the reporting framework” on page 974.
Reporting Framework Configuration	Allows users and members of user groups to administer and configure the reporting framework. See Chapter 29, “Configuring and generating the reporting framework,” on page 951.
Reporting Periods	Allows users and members of user groups to finalize and reapply Reporting Periods. Finalize allows users and members of user groups to finalize the active Reporting Period. Reapply allows users and members of user groups to reapply the active Reporting Period (Standard UI only). For more information, see Chapter 18, “Reporting periods, object resets, and rulesets,” on page 577.
Reporting Schema	Allows users and members of user groups to manage the Reporting Schema. See Chapter 6, “Managing the reporting schema,” on page 159.

Table 51. Administration application permissions (continued)

Permission	Description
Role Templates	Allows users and members of user groups to view, add, and manage roles through the  > Users and Security > Role Templates menu item in the Task Focused UI and the Administration > Role Templates menu item in the Standard UI.
Rules Engine	Allows users and members of user groups to view, create, and manage rules in the Rules Engine . If you are using the Thomson Reuters connector, users access the Rules Engine through the TRRI Rules Engine link on the Regulatory Compliance > TRRI Regulatory Events page. If you are using the Wolters Kluwer connector, users access the Rules Engine through the Wolters Kluwer Rules Engine link on the Regulatory Compliance > WK Regulatory Events page in the Task Focused UI.
Scheduler	Allows users and members of user groups to create and manage scheduled jobs through the  > Solution Configuration > Scheduler menu item in the Task Focused UI.
Search	Allows users and members of user groups to manage and maintain global search operations through the Administration > Global Search menu item in the Standard UI. For more information, see Chapter 20, “Configuring the global search feature,” on page 649 .
Security Rules	Allows users and members of user groups to manage and maintain security rules. For more information, see “Security rules” on page 120 .
Security Scorecard Feed	Allows users and members of user groups to configure and run the SecurityScorecard job in the Scheduler. The job imports data from SecurityScorecard.
Settings	Allows users and members of user groups to view and manage settings. For more information, see Chapter 19, “Viewing the Configuration and Settings page,” on page 597 .
Solutions	Allows users and members of user groups to use the  > Solution Configuration > Solutions menu item in the Task Focused UI. Allows users and members of user groups to use the  > Solution Configuration > Themes menu item in the Task Focused UI.
SupplyWisdom Feed	Allows users and members of user groups to configure and run the import of Supply Wisdom data by using the SupplyWisdom job in the Scheduler.

Table 51. Administration application permissions (continued)

Permission	Description
Task Focused UI	Allows users and members of user groups to create and manage views in the View Designer. This permission also controls whether the  > Other > Display debug info menu item is displayed. For more information, see “Using the View Designer” on page 385.
TRRI Feed	Allows users and members of user groups to configure the import of Thomson Reuters Regulatory Intelligence (TRRI) data through the  icon on the Regulatory Compliance > TRRI Regulatory Events page in the Task Focused UI.
Watson Assistant	Allows users and members of user groups to use the  > Integrations > Watson Assistant menu item in the Task Focused UI.
Watson Language Translator	Allows users and members of user groups to use the  > Integrations > Watson Language Translator menu item in the Task Focused UI.
WK Feed	Allows users and members of user groups to configure the import of Wolters Kluwer data through the  icon on the Regulatory Compliance > WK Regulatory Events page in the Task Focused UI.
Workflow	Allows users and members of user groups to create workflow definitions and terminate workflow instances through the  > Solution Configuration > Workflows menu item in the Task Focused UI. For more information, see Chapter 15, “Configuring GRC Workflow ,” on page 495.

IBM CommandCenter Studio permissions

This application permission allows users and members of user groups to access Cognos Analytics from IBM OpenPages with Watson.

Table 52. IBM Command Center Studio permission

Permission	Description
Cognos Analytics	In the Task Focused UI, this application permission enable access to IBM Cognos Analytics through the Analytics link in the primary menu. In the Standard UI, this application permission enables the Reporting > Cognos Analytics menu item. Use IBM Cognos Analytics to access your Cognos software and corporate data. Depending on your access permissions, you can create, update, run, and distribute reports, dashboards, stories, and cubes, create and run agents, or schedule entries.

Audit Trail (Change History) permission

The Audit Trail (Change History) application permission allows users and members of user groups to view historical information about object for the selected Reporting Period.

In the Task Focused UI, users can access the **Activity** tab in Task Views.

In the Standard UI, users can select the **Change History** option on the object's detail page.

For more information, see [“Reporting period interactions” on page 578](#) and the *IBM OpenPages with Watson User Guide*.

Note:

- When you copy objects, change histories are not copied with the object. The copy of the object has no change history because it is a new object.
- When you add new fields to an object type, the OpenPages with Watson administrator might see a blank to blank change in the change history because the fields were not previously available.

Browse Files permission

This application permission allows users and members of user groups to view and go to the **Browse** menu item on the **My OpenPages > Attachments** menu in the Standard UI.

This permission applies to the Standard UI only.

Folders permission

This application permission enables users and members of user groups to create new folders in the object repository that do not correspond to business entities. This allows users to create their own folder structure.

This permission applies to the Standard UI only.

Issues permission

This application permission allows users and members of user groups to view the list of Issues through the **Issues** menu item on the **Remediation** menu.

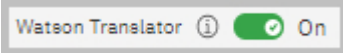
Note: This application permission is in effect only for customers who upgraded or migrated and who have not yet migrated their access controls to the role-based security model. For new, first-time installations, this permission is not honored.

Project Management permission

If your system is configured to enable Project Management, this application permission allows users and members of user groups who are assigned role templates that include the permission to use the Milestone and Milestone Action Item Project Management capabilities.

User interfaces permissions

- **Login to Task Focused UI:** All users have access to the Task Focused UI regardless of whether this permission is enabled. You must set the **Login to Task Focused UI** permission to enabled only for users who also access the Standard UI. This ensures that the URL launches the Task Focused UI.
- **Standard:** Users with the **Standard** permission can access the Standard UI in addition to the Task Focused UI.
- **Watson Assistant UI:** Users with this permission have access to the user interface that enables them to interact with IBM Watson Assistant in OpenPages.

- **Watson Language Translator UI:** Users with this permission can use IBM Watson Language Translator to view translated text in Task Views by using the  icon. It also allows access to the  icon from administrator tasks.

View Locks permission

Users with the View Locks permission can view the existing locks on objects. The View Locks permission does not grant the right to lock or unlock an object - for that you need either the Lock permission or the Unlock permission.

Application permissions not contained under the SOX heading

Some application permissions are not contained under the SOX permission heading, but still have an impact on OpenPages with Watson application behavior. Application permissions determine what functional areas and administrative operations a user or group is able to perform. Typically, users do not require these application permissions.

Users are generally granted the applicable permissions by being assigned to role templates that include those permissions.

All permission

Grants users and members of user groups all permissions and access to every functional and administrative area within OpenPages with Watson (web and server).

Administration permissions

The Administration permissions grant users and members of user groups the ability to archive and restore document versions and to enable and disable System Admin Mode.

Table 53. Administration permissions	
Permission	Description
Archive Management	Allows group members to archive and restore document versions.
System Administration Mode	Allows group members to enable and disable System Admin Mode and perform certain administrative functions. For details see, “Enabling and disabling System Admin Mode” on page 71.

API permissions

This permission enables users to run tools and utilities that use the REST API.

Table 54. API permissions	
Permission	Description
Administration > Background Process > Get Process Info	Required to run ObjectManager operations. To run load, validate, and batch operations with ObjectManager, users also need the SOX > Administration > ImportConfiguration permission. To run dump operations with ObjectManager, users also need the SOX > Administration > ExportConfiguration permission.

Table 54. API permissions (continued)	
Permission	Description
Administration > Background Process > Terminate Process	Required to run the following API processes: - In the OpenPages API: <code>ProcessService.terminateProcess</code> - In the OpenPages GRC REST API: <pre>grc/api/processes/{processid}?action=terminate</pre>

Files permissions

This application permission grants all administrative permissions under the Files grouping that are related to managing files and folders.

Table 55. Files permissions	
Permission	Description
Add Folders	Allows group members to create and add new folders.
Cancel Checkout	Allows group members to cancel the file check-out process for associated files that were checked out by others. When a file check-out is canceled, the file is checked back into the system without applying any changes and no new version of the file is created. Restriction: This permission applies only to file attachments (of the SOXDocument object type).
Lock	Allows group members to lock objects, regardless of sign-off or ACL restrictions.
Reassign Primary Association	Allows members of the user group to reassign primary parent associations and view the Make this object Primary icon on the Parent tab of an object, where <i>object</i> is the object type.
Remove All Tree Locks	Allows members of the user group to unlock resources and/or resource subtrees.
Unlock	Allows group members to unlock objects.

Publishing permissions

The **Add Pages** permission grants administrative permissions to make Cognos and jsp reports available from the OpenPages with Watson application user interface.

Table 56. Publishing permissions	
Permission	Description
Add Pages	Allows group members to add reports.

Configure password requirements

IBM OpenPages with Watson supports the use of strong passwords (passwords that include letters, numbers, and symbols).

It also allows administrators to enforce mandatory password changes and other password behavior.

Note: Configuring password behavior in OpenPages with Watson does not apply if you use single sign-on (SSO), such as LDAP or Microsoft Active Directory. Your internal IT policies dictate password behavior within the product.

Configuring password policies

The IBM OpenPages with Watson allows administrators to modify the password policies for the application.

Using the password policies, administrators can enable strong passwords and control whether user passwords must be changed after a certain length of time.

To access the password settings, go to  > **System Configuration** > **Settings** > **Platform** > **Security** > **Password**

Table 57. Password Settings	
Setting	Description
Encryption Administrator	The user name who is allowed to change the password encryption algorithm and the encryption key.
Strong Policies - Character Groups 1-4	These settings allow the administrator to configure the strong password policies for the application. Each Character Group takes a comma-separated list of characters. By default, these groups are empty. If strong passwords are enabled, each password is required to contain at least one character from each group. If a group is empty, that group is ignored. Important: You cannot include the comma as a required character in a strong password.
Strong Policies - Enabled	If the value is set to: • <code>true</code> - then users are required to enter strong passwords when they specify their user password. • <code>false</code> - then users are not required to enter strong passwords when they specify their user password. This value is set by default.
Enabled	Sets whether the password policies are active or not. The default value for this setting is <code>false</code> .
Maximum Length	Sets the maximum length of the password. The default value for this setting is 32.
Minimum Length	Sets the minimum length of the password. The default value for this setting is 6.
Notify Before Days	Sets the number of days before a user's password expires that the user is shown a warning message at logon about their password expiring.

Updating the password encryption algorithm

To update the password encryption algorithm, you use the Update Password Encryption Algorithm (UPEA) tool.

Note: The topics in this section are not applicable in IBM OpenPages for IBM Cloud Pak for Data.

Before you use the UPEA tool, ensure that you complete the following tasks:

- [“Verifying the current encryption algorithm” on page 100](#)
- [“Verifying the environment” on page 100](#)
- [“Configuring the security provider in the java.security file” on page 101](#)
- [“Preparing passwords in the aurora.properties file and the op-backup-restore.env file for reencryption” on page 101](#)
- [“Updating the Users table to change passwords” on page 102](#)

You run the tool from the command line as follows:

<OP_HOME>\bin\UpdatePasswordEncryptionAlgorithm.cmd (Windows)

<OP_HOME>/bin/UpdatePasswordEncryptionAlgorithm.sh (Linux)

Tip: You can also run the tool from a remote system, such as your laptop. For more information, see [“Installing tools and utilities \(IBM OpenPages with Watson\)” on page 824](#)

You can use the UPEA tool to do the following tasks:

- Change the encryption algorithm from 3DES to AES.
- Change the AES encryption key - this is the default encryption algorithm.

Verifying the current encryption algorithm

If you have a legacy system, verify the name of the current encryption algorithm before you run the UPEA tool to change the algorithm to AES as follows.

Procedure

1. Log on to a machine with SQL*Plus and access to the database server.
2. Execute the following SQL statement:

```
select algorithmname from encryptionmodules where inactive=0;
```

3. When you are finished, log out of SQL*Plus.

Results

If the SQL statement returns the name:

- 3DES, then run the UPEA tool to change the encryption algorithm to AES.
- AES, then you already have the AES encryption algorithm. If you want, you can use the UPEA tool to change the AES encryption key.

Verifying the environment

The following tasks must be completed before you run the UPEA tool.

- An IBM OpenPages with Watson system must be properly installed and functioning on the machine.
- A full backup of the OpenPages with Watson database must be completed. For more information, see [Chapter 21, “Using IBM OpenPages with Watson utilities with Db2 databases,” on page 679](#) or [Chapter 22, “Using IBM OpenPages with Watson utilities with Oracle databases,” on page 713](#).
- Ensure that all OpenPages with Watson servers are started and that no users are logged on to the system during the password encryption update.

Note: For details on starting and stopping servers in Windows and Linux environments, see [“Starting application servers” on page 841](#).

Configuring the security provider in the `java.security` file

The security provider must be specified in the `java.security` file.

About this task

Note the following recent name changes:

- `bcprov-jdk14-145.jar` is `bcprov-jdk15to18-1.68.jar` in 8.2.0.2 or later
- `org.bouncycastle145.jce.provider.BouncyCastleProvider` is `org.bouncycastle.jce.provider.BouncyCastleProvider` in 8.2.0.2 or later
- `CAMCryptoBC` is `BC` in 8.2.0.2 or later

These steps use the updated names for 8.2.0.2 and later.

Procedure

Verify that the `BouncyCastleProvider` security provider has been added to the `java.security` file as follows:

- a) Open a command or shell window on the application server.
- b) Go to:

```
<JAVA_HOME>/jre/lib/security
```

Where:

<JAVA_HOME> is the installation location of IBM SDK, Java Technology Edition. For example:

- On Windows: `C:\IBM\java_8.0_64`
- On Linux: `/opt/IBM/java_8.0_64`

- c) Make a backup copy of the `java.security` file before you modify it.
- d) Open the `java.security` file in a text editor of your choice.
- e) Locate the following property in the file:

```
security.provider.<#>=
```

- f) If the `BouncyCastleProvider` security provider is not present, add the following line:

```
security.provider.<#>=org.bouncycastle.jce.provider.BouncyCastleProvider
```

Where: The number sign, `<#>`, is one increment above the last number in the list. For example, `security.provider.9`.

- g) Save and close the file.

Preparing passwords in the `aurora.properties` file and the `op-backup-restore.env` file for reencryption

You can reencrypt the passwords that are in the `aurora.properties` and `op-backup-restore.env` files. By default, the files are in the `<OP_Home>` directory.

For Microsoft Windows operating systems, the default installation directory of OpenPages with Watson is `C:\IBM\OpenPages`.

For Linux operating systems, the default installation directory of OpenPages with Watson is `/opt/opuser/IBM/OpenPages`.

Procedure

1. Open a command or shell window on the application server.

2. Go to the <OP_Home>|aurora|conf directory.
3. Edit the aurora.properties file in the conf directory.
 - a) Make a backup copy of the file.
 - b) Open the file in a text editor of your choice.
 - c) Search the file for properties that include the string password.
 - d) Change all password values after the equal sign to plain text.
 - e) Save and close the file.

Note: The passwords are encrypted when you restart the servers.

4. Edit the op-backup-restore.env file in the <OP_Home>|aurora|bin directory.
 - a) Make a backup copy of the file.
 - b) Open the file in a text editor of your choice.
 - c) Search the file for properties that include the string PWD.
 - d) Change each password value to plain text.
 - e) Save and close the file.

Note: The passwords are encrypted when you restart the servers.

Updating the Users table to change passwords

Updating the Users table to change passwords with the UPEA tool applies only to upgraded databases.

Procedure

1. On a computer that has access to the database server, connect to the OpenPages database as the OpenPages database user.
2. Run the following SQL statement to update the Users table so that passwords can be changed:

```
update users set flag_can_change_password=1 where actorid not in (select actorid from
actorinfo where name = 'OPSystem');
```

UPEA tool syntax and parameters

The UPEA tool defines the parameters of the password encryption algorithm.

UPEA syntax

The syntax of the UPEA tool is detailed in the following section:

```
UpdatePasswordEncryptionAlgorithm
-Mode [CA|CK]
-AlgorithmName [AES]
-ProviderName BC
-ProviderClass org.bouncycastle.jce.provider.BouncyCastleProvider
-Username <OpenPagesAdministrator>
-Password <OpenPagesAdministrator password>
[-KeySize 128]
[-?]
```

Note the following recent name changes:

- bcprov-jdk14-145.jar is bcprov-jdk15to18-1.68.jar in 8.2.0.2 or later
- org.bouncycastle145.jce.provider.BouncyCastleProvider is org.bouncycastle.jce.provider.BouncyCastleProvider in 8.2.0.2 or later
- CAMCryptoBC is BC in 8.2.0.2 or later

This topic uses the updated names for 8.2.0.2 and later.

The following table describes the parameters of the UPEA tool.

<i>Table 58. UPEA parameters</i>	
Parameter	Description
-Mode	Required. Use to specify the mode in which the tool should run. Possible modes are: • CA (for Change Algorithm) — used to switch the encryption algorithm from 3DES to AES. • CK (for Change Key) — used to change the AES encryption key.
-AlgorithmName	Required. Use to specify the type of encryption algorithm to use. The only valid value is AES.
-ProviderName	Required. Use when you change algorithms to the AES encryption algorithm only. Has only one valid value: BC.
-ProviderClass	Required. Use only in conjugation with -ProviderName to specify the class for the new encryption algorithm. Has only one valid value: org.bouncycastle.jce.provider.BouncyCastleProvider
-Username	Required. Use to specify the user name to use when you modify the user passwords. Must be the same as the user specified in the OpenPages Platform Security Password Encryption Encryption Administrator setting.
-Password	Required. Use to specify the password to the Encryption Administrator account.
-KeySize	Optional. Use to specify the length of the AES encryption key. The only valid value is 128. If an invalid value is given, or no value is provided, the default value of 128 is used.
-?	Optional. Displays the on-screen help for the UPEA tool.

Changing the password encryption algorithm to AES

You can run the UPEA tool to change the password encryption algorithm from 3DES or OP-CUSTOM to AES, which is more secure. To do this task, you must be an Encryption Administrator.

Procedure

1. Edit the <OP_HOME>/aurora/conf/aurora.properties file and the <OP_HOME>/aurora/bin/op-backup-restore.env file and change any encrypted passwords to plain text.

- If you are using 3DES, look for lines that contain {3DES}.

For example, suppose the aurora.properties file contains the following line:
database.PASSWORD={3DES}Rj+steg+3eU7kb80+\=\=. The database password is encrypted with the 3DES algorithm. Replace the encrypted password with the password in plain text, for example, database.PASSWORD=db_password.

- If you are using OP-CUSTOM, the lines do not have an algorithm indicator. Look for encrypted passwords and change each of them to the password in plain text.

The passwords are encrypted with the AES algorithm when you restart the OpenPages with Watson services in step 3.

2. Open a command or shell window on the OpenPages application server.

Go to the <OP_HOME>/bin directory.

From the command or shell window, run the following command on a single line:

```
UpdatePasswordEncryptionAlgorithm.sh|.cmd -Mode CA -AlgorithmName AES  
-ProviderName BC  
-ProviderClass org.bouncycastle.jce.provider.BouncyCastleProvider -KeySize 128  
-Username <OpenPagesAdministrator> -Password <OpenPagesAdministratorPassword>
```

3. Restart all OpenPages services.
4. If you are using OpenPages to authenticate users, notify all users that their passwords have been reset to 0p3nP4g3s and that they must change their passwords the next time they log into the system.

Note: If you are using Single Sign-On (SSO), LDAP, or another external system to authenticate users, passwords are not reset.

Changing the AES encryption key

At certain times, you might want to change the encryption key that is used by the AES encryption algorithm. You can change the encryption key by using the UPEA tool. To do this task, you must be an Encryption Administrator.

Procedure

1. Log on to the IBM OpenPages with Watson server as a user with administrative privileges.
2. Open a command or shell window and change directory to the <OP_Home>/bin directory.
3. From the command or shell window, run the following command on a single line:

Windows

```
UpdatePasswordEncryptionAlgorithm -Mode CK -AlgorithmName AES  
-Username <OpenPagesAdministrator> -Password <password>
```

Linux

```
./UpdatePasswordEncryptionAlgorithm.sh -Mode CK -AlgorithmName AES  
-Username <OpenPagesAdministrator> -Password <password>
```

Where: <password> is the password for the OpenPagesAdministrator account.

4. Restart OpenPages with Watson services for the changes to take effect.

Chapter 5. Security

Most of your security requirements can be handled in IBM OpenPages with Watson with folder-based security, either role-based security or custom security. If you need to refine folder-based security, use security rules.

Role-based security

Use role-based security to define application permissions for each role and to set access control (Read, Write, Delete, Associate) for each object that is included in that role. All users in each role inherit the same security access controls.

Custom security

Use custom security to set access control (Read, Write, Delete, Associate) on folders for Project Milestones and Project Action Items. All objects in the folder inherit the same security access controls.

Note: The custom security feature is deprecated. Use role based security instead.

Security rules

You can define two types of security rule:

- Record level security rules

Use record level security rules to control access to individual objects in a folder. For example, two GRC domains share a common organizational hierarchy. They share some common object instances, such as processes, but they do not want to share other object instances, such as risks and controls. If you do not create security rules on objects, folder-based security applies.

Record level security rules have the following access controls: Create, Read, Update, Delete, and Associate. The Write access control in folder-based security is split into Create and Update for security rules, which gives you more control over what users can and cannot do.

- Field level security rules

Use field level security rules to control access to individual fields within an object.

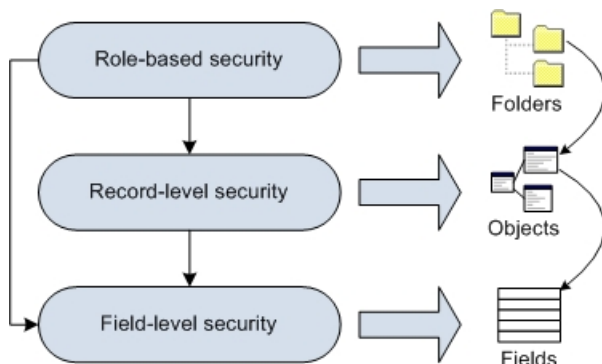


Figure 4. Levels of security

Role-based security and security rules differ from profiles and field dependencies because security is applied everywhere rather than in the OpenPages with Watson application only.

Role-based security model

A role-based security model provides a way for administrators to control user and group access to objects that are under a defined security point within the object hierarchy according to the role the user or group is expected to perform within the organization.

Typical security points are business entities, processes, or sub-processes (can also be set at lower security point levels if wanted).

Figure 5 on page 106 shows how various users and groups can have different permissions set for accessing business entities (a defined security point in the object hierarchy) and objects that are under a specific hierarchy.

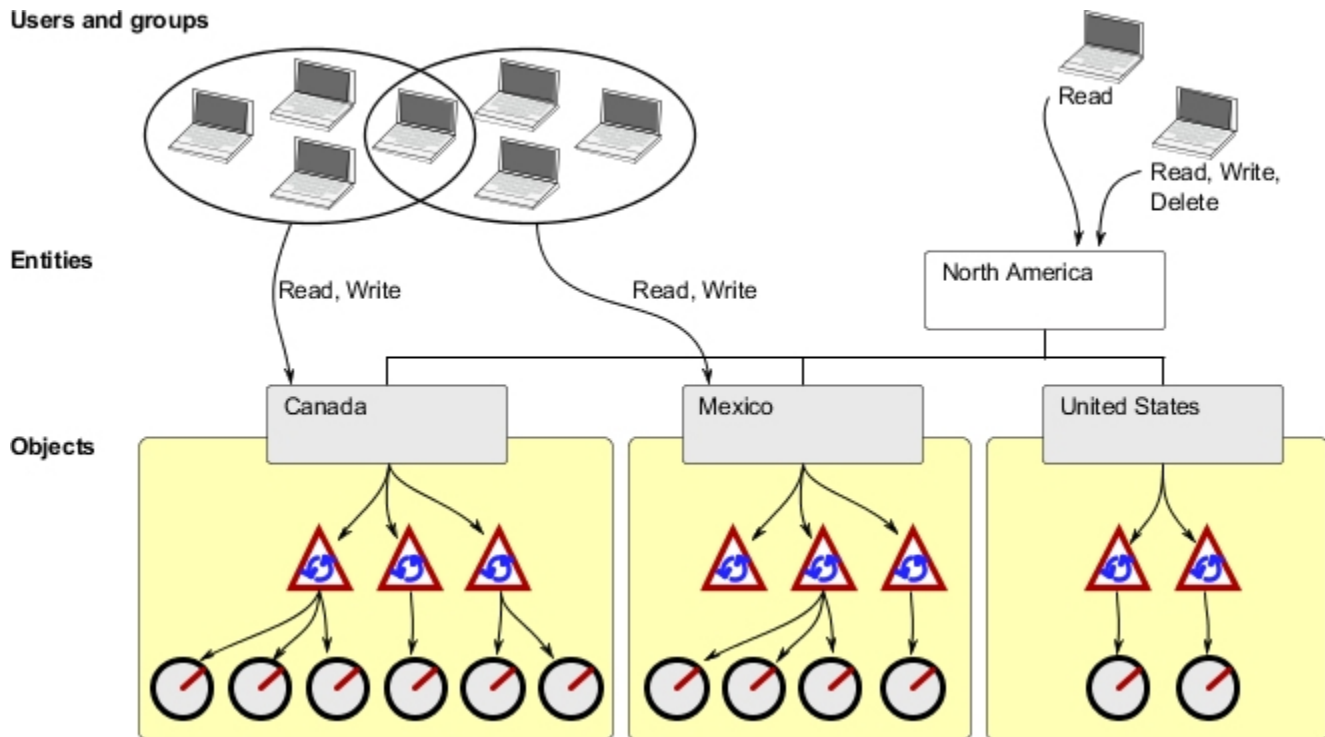


Figure 5. Security concepts in a hierarchy

Based on the type of security context points defined in your security model, such as Business Entity, Process, Control Objective or Risk Assessment, you can use a role template to define a set of permissions for a set of object types.

For each role template that you define, you can set the following:

- Access control (Read, Write, Delete, Associate) for each object type included in that role. For details, see [“Role-based access control permissions”](#) on page 111.
- Application permissions for the role. For information about the various application permissions, see [“Defining application permissions”](#) on page 90.

Important: These application permissions do not include administrative group and user security management permissions, such as resetting passwords, assigning roles, adding users, and so forth. To learn more about assigning group and user security management permissions to administrators, see [“Delegate administrator permissions”](#) on page 76.

By assigning a role (an instance of a role template) to a user or group at specific security context point in the object hierarchy, you can control access to objects. *Roles* represent the usual or expected function that a user or group plays within an organization. Some examples of roles are: Finance Reviewer, Tester, External Auditor, System Administrator, Control Owner, Risk Assessor.

When you assign a role to a group or user, the security settings of that role template are acquired by that group or user and permissions are automatically granted, per the role template definition, to all objects below the specified security point.

For example, if a role were assigned to a user for a business unit (security context point), access control for specific object types under that security point would be set in the object hierarchy. Object types that were excluded from the role would be hidden from view, object types that were included would be visible and could be accessed by users and groups assigned to that role.

So that you can have a clear and accurate understanding of which users and groups have access to what and with which permissions, and what access control modifications were made in the system, you can run

a variety of reports to view this data. For details on the types of configuration audit and security reports available to you, see the section [“Audit Reports folder”](#) on page 168.

Security context points

The structure of the object hierarchy that is defined in your system also acts as the security context point to which access control can be assigned.

Roles (defined by role templates) are granted to specific security points in the object hierarchy, and permissions for a particular role are automatically granted to all objects that are created in the same location beneath that security point. If a role is assigned to a group on a top-level Business Entity, then all users of that group would have access to that business entity and would be able to access all objects under that entity as per the permissions in the role.

By default, the installation process automatically sets Business Entity (SOXBusEntity) as the security context point within the object hierarchy at which roles can be assigned.

Example

You have a regional office called North America and a sub-regional office called United States. When you create the business entity, the folder structure /BusinessEntity/North America/United States would automatically be created.

You also created a role template called Entity Owners that has access defined for the following object types:

- Business Entity
- Process
- Sub-process
- Control Objective
- Risk
- Control

When you assign the Entity Owners role template to the United States business entity, the following structure is automatically generated under the root folder of each object type:

```
/Processes/North America/United States  
/Sub-processes/North America/United States  
/ControlObjectives/North America/United States  
/Risks/North America/United States  
/Controls/North America/United States
```

Note: that the folder structure /BusinessEntity/North America/United States does not have to be generated since it already exists (was automatically created when the business entity was initially created).

Figure 6 on page 108 shows how access permissions (R=Read, W=Write, D=Delete, A=Associate) can be granted to specific objects in the hierarchy under the United States business entity security context point.

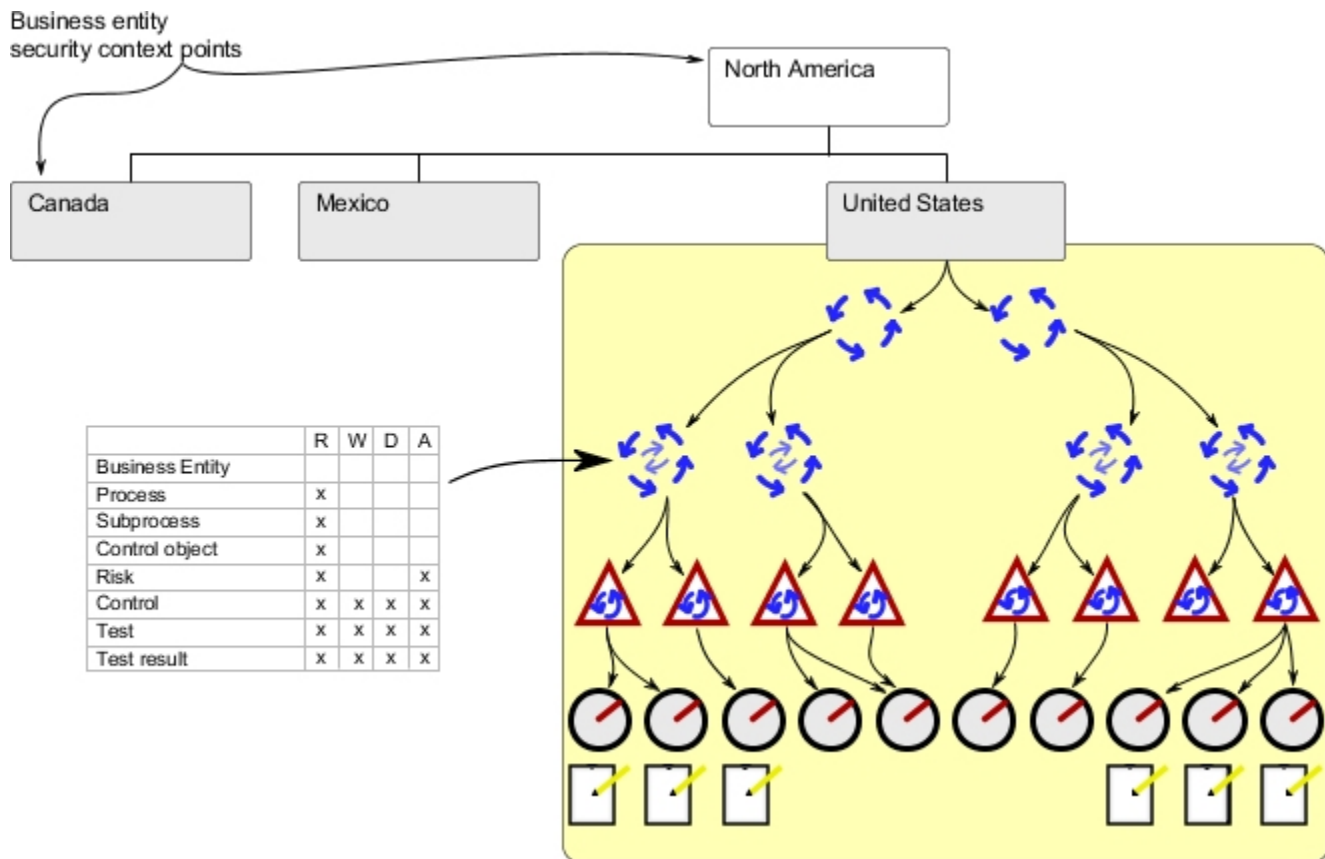


Figure 6. Business entity security context points

For details on assigning security management permissions to security domain group administrators, see [“Delegate administrator permissions”](#) on page 76.

Extending security context points

To achieve a finer level of control, it is possible to extend the security context point to other objects in the hierarchy (such as Business Entity-Process or Business Entity-Risk Assessment).

To achieve more control, change the Model setting. For more information, see [“Set the system security model”](#) on page 635).

Note: The Model setting is a system-wide setting. Switching the security model after data is loaded (or migrated) into the system is not recommended and requires assistance from IBM OpenPages with Watson Services.

To determine the optimal security context points for your organization, you need to evaluate your requirements for securing resources at lower security context points in your hierarchy. Extending the security context points to achieve a finer level of control does not prevent you from defining security at higher security context points.

Example

You extended the security context points to include Business Entity-Process. In this scenario, administrators could assign, for example, a "Process Role Template" to one or more users or groups on one or more Processes.

Permissions (Read, Write, Delete, Associate) in the "Process Role Template" could then be assigned to that Process security context point. The permissions in that template are applied to every object created beneath that point in the object hierarchy and to any object that is created in the future below that point.

Although users and groups who are assigned the "Process Role Template" would be able to navigate to and access Processes and child objects beneath a Process hierarchy, the details of the parent Business Entity would be hidden from them.

Note: Users who have roles that are assigned to a context security point within the Business Entity level only have only navigation access to the parent Business Entity. If users require the ability to view or modify the details of a parent Business Entity, then you must use an entity-based role template to grant explicit Read and/or Write permission to users at an entity security point.

The user interface in OpenPages with Watson does not allow breaking folder ACL inheritance on any folder on which role-based access control is assigned. Administrators are strongly advised not to break folder inheritance using ObjectManager or any other application interfaces on any object type folders as this will cause role-based security to fail.

Figure 7 on page 109 shows how access permissions can be granted when the security context points are extended to include Process objects as security points to achieve a higher level of control.

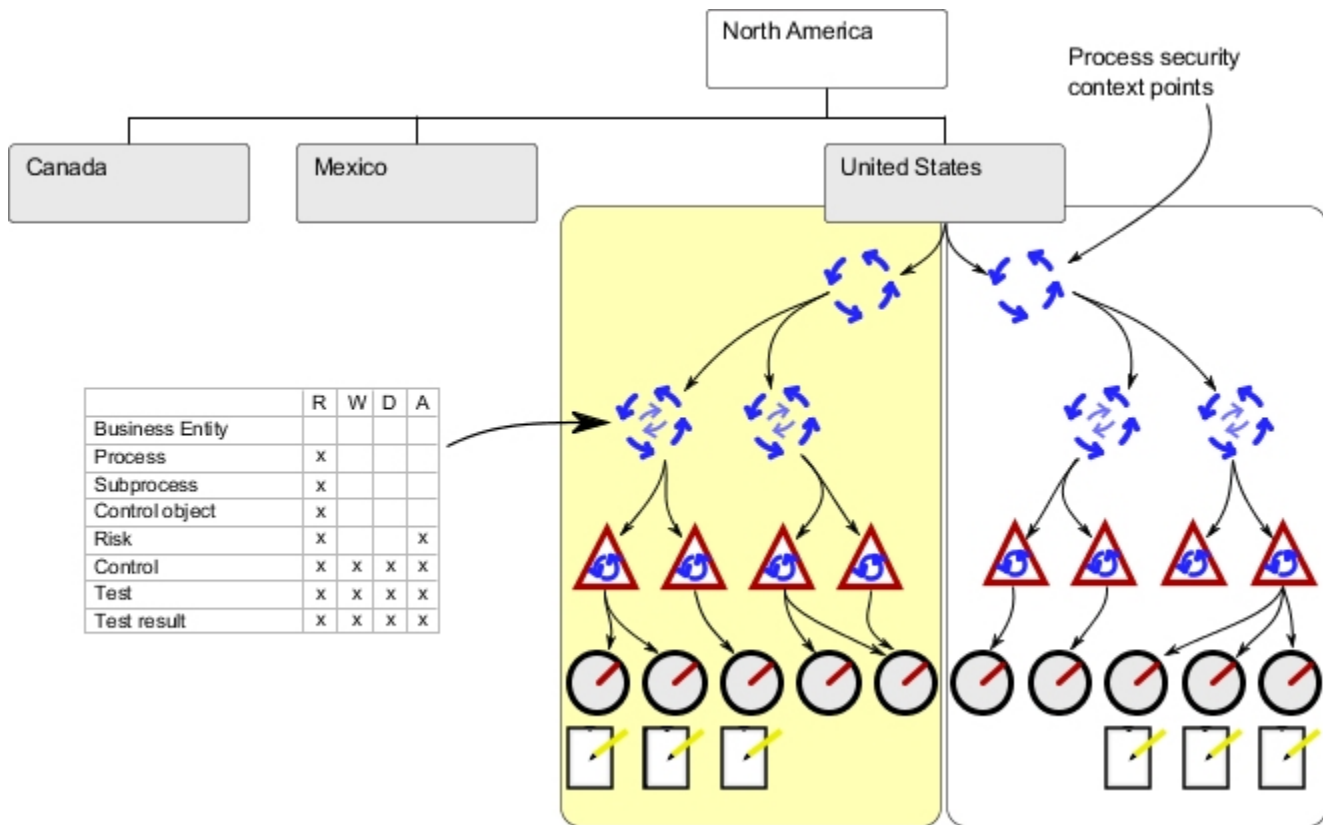


Figure 7. Business entity and process extended context points

Reporting framework and multiple security context points

In a security model that contains multiple security context points, objects that form a "triangle" relationship have implications for the reporting framework.

Triangle relationships are formed among objects when an object type is configured to have a parent of more than one type (typically, the second parent is a recursive object type).

For example, if Risk object types are configured to be a child of Process and a child of SubProcess object types, then a triangle relationship will exist among these different object types. Figure 8 on page 110 shows an example of a triangle relationship between a child Risk and parent Process and Sub-Process object types.

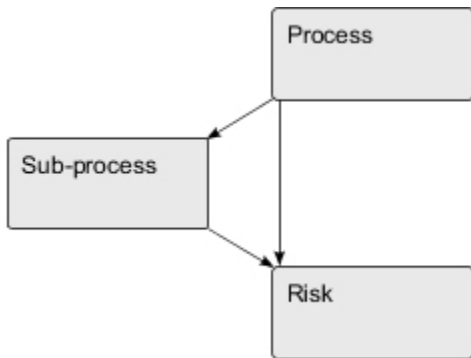


Figure 8. Triangle relationship between different object types

In the reporting framework, fields from parent objects within a triangle relationship (for example, Process and Sub-Process) are stored in the same Query Subject along with the ID of the shared child object (such as, Risk ID). When both Process and Sub-Process fields are part of the same Query Subject, a user would require Read permission on both Process and Sub-Process object types to view these fields in a report.

When a triangle relationship exists among objects, avoid the use of the Sub-Process (or similar) object type as a security point in your system unless you are willing to always grant Read access to the parent object type (such as Process).

Note: For information about configuring triangle object relationships in the reporting framework, see [“Triangle object relationships” on page 955](#).

Sample scenario

A user has Read access for Sub-Process object types, so they can view details for Sub-Process objects in the application user interface.

If the same user does not have Read or Write access to the parent Process and Business Entity, that user will still have an implicit Navigate permission to the Process and Business Entity object types. The implicit Navigate permission allows users to navigate through the object hierarchy from, for example, an Overview page to object types that are lower in the hierarchy (such as Sub-Process) for which they have explicit permission (in this case, Read access).

If a triangle relationship exists among these object types, the same user would not have permission to view the Sub-Process detail in a report unless the user was also granted explicit Read access on the Process object type (as SUBPROCESSES and PROCESSES reside in the same Query Subject).

Security domains

In IBM OpenPages with Watson, special user groups, called "security domain groups", are automatically created when a Business Entity or Sub-entity object is created.

Security domain groups act as containers for users and organizational groups associated with that business entity.

In the  > **Users and Security** > **Domains & Groups** task in Task Focused UI, each security domain group is located under a top-level (root) **Security Domains** folder. The name of the group corresponds to the name of the business entity to which it belongs.

In the Standard UI, each security domain group is identified by a people hierarchy icon  under a top-level (root) **Security Domains** folder on the Users, Groups and Domains page, and the name of the group corresponds to the name of the business entity to which it belongs.

Users in a security domain group are generally assigned roles to work on the objects under that entity. You can also delegate specific security management activities to administrators in a security domain group for managing users and groups within that business entity.

Note: When you expand a security domain group, only child security domains are displayed. Any organizational groups and users associated with that security domain can be viewed only from the detail page of that security domain group.

Example

You want to delegate the security activity of resetting passwords to an administrator for members of a particular Sales Office security domain group.

You would navigate to the detail page of the Sales Office security domain group and assign the "Reset Password" permission to an administrator. That administrator would then be able to only reset passwords for users in that Sales Office security domain group. You could repeat this process of delegating "Reset Password" permission to an administrator for each security domain group within your organizational hierarchy.

Moving business entities

On occasion, you may need to reorganize your business entity structure by moving a Business Entity with its corresponding object hierarchy from one location to another.

When you move a business entity structure, all role assignments that were made on that business entity remain intact.

This means that users and groups who were granted various roles at a specific Business Entity security context point before the move operation, will continue to have the same roles and access after the move operation.

Note: If you are planning on moving a large object hierarchy, consider using the Entity Move/Rename utility that is included with IBM OpenPages with Watson. This utility allows batch processing of multiple Business Entities for overnight or weekend execution without running the risk of operations timing out. You can run the utility interactively or as a scheduled job. See the *Entity Move/Rename Utility ReadMe* for details.

Copying business entities

If you use the copy operation to expedite the setup of child business entities by duplicating an instance of an existing business entity, a security domain group for that new child business entity is automatically created by the system and is associated to the security domain group of the parent business entity.

Initially, the new security domain group that corresponds to the new child business entity is empty (no users or groups). However, users and groups who have assigned roles with access control defined for the parent business entity will have the same access on the new child business entity.

An administrator of the security domain group for the parent business entity can add and/or associate users and groups to the security domain group of the new child business entity. An administrator of the parent business entity can delegate administration activities by selecting an administrator. For details, see [“Delegate administrator permissions” on page 76](#).

To refine user access to the new child business entity, you can use the application interface to define role templates and grant roles to users and groups. For details, see [“Role templates” on page 113](#).

Role-based access control permissions

When you create a role template, you can specify the type of security access control that you want to have on an object type's folder structure for groups and users who are assigned to that role.

Note:

- The file (SOXDocument) and link (SOXExternalDocument) object types have the same root storage folder path. As a result, you can configure only one set of ACLs for both these object types in a role.
- Role-based security does not apply to Project Milestones and Project Action Items. For details on setting security access for these object types, see [“Custom security for projects” on page 144](#).

- Any new object types that are added to the system are excluded from all existing role templates.

Access control permissions for role-based security

For each object type that you want to include in a Role Template, you can set access control (ACL) permissions on the object's folder structure.

- **Read** - when you select an object type for inclusion in a role, the value of the Read permission is automatically set to Granted on the object's folder structure. This means that any groups or users assigned to this role can navigate to, and view the details of objects (parent and child) contained in the folder and the folder itself, but cannot modify any object data unless other permissions are explicitly set.
- **Write** - the groups or users assigned to this role can read and modify the details of objects within the selected folder, but cannot delete objects. Write access to a folder is required for creating new objects within the folder.
- **Delete** - the group or user assigned to this role can read, modify, and delete objects within the folder structure.
- **Associate** - the group or user assigned to this role can create associations between objects.

For each ACL permission, you can set an explicit value. These values or settings are propagated downward and inherited by any child object storage folders under that parent object's folder structure.

For each ACL permission, you can set one of the following values:

Note: For usage examples, see [“Scenarios: Using access control settings” on page 112](#).

- **Unspecified** - by default, no access is explicitly granted to the user or group for the corresponding object through this role. The "Unspecified" setting does not override any access that is granted on this object through other roles or access inherited through a role on higher level security context points. This value should be used instead of "Denied" since it is less restrictive.
- **Granted** - this explicit setting gives a user or group full access to the specified action (Write/Delete/Associate). The user can modify, or delete the file or folder, depending on the permission.
- **Denied** - this explicit setting does not allow a user or group to perform the specified action (Write/Delete/Associate). The "Denied" setting overrides any access that is granted on this object through other roles or access inherited through a role on higher level security context points.

Scenarios: Using access control settings

The following case scenarios provide examples of how the system may respond with various settings.

Scenario 1: Using explicit settings

If a user or group is assigned multiple roles and the explicit ACL settings within these roles conflict, the most restrictive explicit setting will be used.

For example, we create a Test Performer and a Test Reviewer role for the Test object type. Each role has the **Write** ACL permission explicitly set to the following:

- Test Performer has **Write = Granted**
- Test Reviewer has **Write = Denied**

If we assign both roles (Test Performer and Test Reviewer) to a user called Tester1, Tester1 will not be able to create new Test objects even though the Test Performer role has Write = Granted. This is because the Write = Denied permission of the Test Reviewer role is more restrictive than the Write = Granted permission, and the most restrictive setting is automatically applied.

Scenario 2: Using explicit and unspecified settings

If a user or group is assigned multiple roles and one role has an explicit ACL settings but the other role has Unspecified for the same permission, the explicit setting will be used.

For example, we create an Initial Test and a Final Test role for the Test object type. The roles have the **Write** ACL permission set to the following:

- Initial Test has **Write = Granted**
- Final Test has **Write = Unspecified**

If we assign both roles (Initial Test and Final Test) to a user called Tester1, Tester1 will be able to create new Test objects even though the Final Test role has Write = Unspecified. This is because the Write = Granted permission is explicit and the explicit setting is automatically applied.

Scenario 3: Using unspecified settings

If a user or group is assigned a single role and the ACL settings within this role:

- Use the default value Unspecified, and
- No other access control has been explicitly set for the user or group

then access is DENIED.

For example, we create an Initial Test role for the Test object type. The role has the **Write** ACL permission set to the following:

Initial Test has **Write = Unspecified**

If we assign the role (Initial Test) to a user called Tester1 and Tester1 has not been granted access through any group-inheritance, Tester1 will not be able to create new Test objects.

Role templates

Role templates are global to the application and are available for role assignment by any administrator of a security domain who has the **Assign Roles** administrator permission.

Because the **Assign Roles** permission is a global permission, it is not constrained by the hierarchy of the role. Users who are granted this permission can manage any role in the system.

Role templates are the preferred method for granting users or groups application permissions.

Note:

- Both application permissions and ACLs are included in the role definition process. When a role is assigned to a user or a group on any business entity or security context point, that user or group automatically acquires the application permissions defined in that role template.
- When a user or group is assigned multiple roles, the user or group accumulates the application permissions that are defined in the various roles. Application permissions are granted by the role (not the security context point) and apply in all situations where the user has the correct ACL access. For example, users with Read permission to Business Entities and the **Audit Trail** application permission will be able to view the Change History (audit trail) for those Business Entities.

Accessing Role Templates

You can define application permissions by using role templates.

Before you begin

Only a Super Administrator or a delegated administrator with the **Role Templates** permission can access Role Templates.

About this task

Role Templates can be managed using tasks in either the Task Focused UI or the Standard UI. Changes made in one interface are immediately reflected in the other.

Note: When you perform an action on a role template (such as creating, editing, assigning, enabling or disabling) using the Standard UI, the role template is automatically locked by the system to prevent other users from simultaneously accessing the template. After you save your changes (or cancel the operation), the Role Template is unlocked. If the session times out before you are able to finish modifying a role template, an **Unlock** icon is displayed on the detail page of the role template. To unlock the role template and resume your editing activity, click the **Unlock** icon.

When you perform an action on a role template (such as creating, editing, assigning, enabling or disabling) using the Task Focused UI, the role template is not locked.

Procedure

1. Click  > **Users and Security** > **Role Templates**.
Or, in the Standard UI, click **Administration** > **Role Templates**.
2. From the list of **Role Templates**, you can add, view, and modify role templates.

Adding a role template (Task Focused UI)

You can add a role template to define application permissions.

Before you begin

Ensure that System Admin Mode is disabled.

About this task

The role template page guides you through creating a new role, selecting object types for inclusion or exclusion, and setting security on the selected object types.

Role template names are not localizable.

Note: Users who have roles that are assigned to a context security point within the Business Entity level only have only navigation access to the parent Business Entity. If users require the ability to view or modify the details of a parent Business Entity, then you must use an entity-based role template to grant explicit Read and/or Write permission to users at an entity security point.

Procedure

1. Click  > **Users and Security** > **Role Templates**.
2. Click **New Role Template**.
3. In **Name**, type a name for the role. For example, `Tester01`.
4. Optional: In **Description**, type a brief description of this role.
5. In **Role Type**, select the type of security context point you want from the list.

Note: If only one security context point type (such as Business Entity) is defined for your system, this is the only value in the list. Security context point types are derived from the security model that is in effect for your installation.

6. Click **Add**.
7. In the **Role Access Controls** section:
 - a) Click **Add** to assign object types to the role template.
 - b) Select the check box next to each object type for which you want to configure folder permissions. For example, if you wanted to configure permissions for Risk and Issue objects, you would select *Risk* and *Issue*.
Note: Use Search, if needed. To select all object types, select the check box in the **Name** column.
 - c) Click **Add**.
After you assign the object type, you can assign permissions using a table format.

- d) Click a row (or click the check box and click **Edit**) for an object type and select a setting value for each permission (Write, Delete, and Associate). By default, Read is always set to Granted, and all other permissions are set to Unspecified.

For setting details, see [“Role-based access control permissions” on page 111](#).

- e) Click **Done**. Repeat for other object types.

8. In the **Role Permissions** section:

- a) Click **Edit**.
- b) Select the application permissions that you want to assign to this role template. For a description of the various application permissions, see [“Types of application permissions” on page 91](#).
- c) Click **Done**.

The new role is listed on the **Role Permissions** section.

9. To assign the role to a user or group, see [“Assigning and removing a role from a user or group \(Task Focused UI\)” on page 117](#).

Modifying a role template

When you modify a role template after you assign it to users and/or groups, any changes you make to access control (ACLs) and application permissions are automatically propagated to those users and groups.

You can use this propagation feature to grant additional access control or revoke access control on certain object types to existing users and/or groups, by modifying the role template.

Typically, a Super Administrator or a top-level security domain administrator (with **Assign Roles** administration permission and **Role Templates** application permission) are able to modify, disable or delete a Role Template. This is because a lower-level security domain administrator, though having **Role Templates** application permission, does not have **Assign Roles** administration permission on higher-level entities and hence is not able to successfully edit, disable, or delete a template.

Procedure

1. Click  > **Users and Security** > **Role Templates**.
Or, in the Standard UI, click **Administration** > **Role Templates**.
2. From the list of Role Templates, click the name of the role you want to modify.
3. On the detail page of the selected role, click **Edit**.
4. Make the required changes.
5. Click **Done**.

Enabling and disabling a role template

You can make a role inactive and keep it for future use by disabling the role. You can also enable a role that was previously disabled.

Procedure

1. Click  > **Users and Security** > **Role Templates**.
Or, in the Standard UI, click **Administration** > **Role Templates**.
2. From the list of Role Templates, click the name of the role you want to enable or disable. The detail page of the selected role is displayed.
3. Click **Disable** or **Enable**.

Results

When you disable a role, the following occurs:

- Depending on the **Disable Role Group** application setting, any users and groups, who were previously assigned that role, either retain or lose their access control and application permissions. By default, the setting allows users and groups to retain access after a role is disabled. For more information, see [“Disable access control on Role groups” on page 636](#).
- The disabled role template is removed from the role assignment selection list and cannot be used for further role assignments.
- The status of the role on **Role Templates** changes from Active to Inactive.

When you enable a role, the following occurs:

- Any users or groups who are assigned that role are able to perform activities on objects that are associated with that role.
- The enabled role template is included in the role assignment selection list and can be used for further role assignments.
- The status of the role on **Role Templates** changes from Inactive to Active.

Deleting a role template

To automatically revoke all role assignments, you can delete a role template.

An administrator (or Super Administrator) with **Role Templates** application permission and the **Assign Roles** administrator permission can assign and/or revoke roles on any entity in the system. Only a Super Administrator or a top-level entity administrator is able to delete role templates, since this action automatically revokes all role assignments that were made using the selected role template on any business unit in the application.

When you delete a role, the following occurs:

- Any users or groups who were assigned that role are no longer able to perform the activities on objects that are associated with that role.
- The role is permanently removed from the list of roles on the **Role Templates** tab and cannot be restored.

If you want to remove a role without deleting it, you can disassociate the role instead by revoking the role from the user or group.

Procedure

1. Click  > **Users and Security** > **Role Templates**.

Or, in the Standard UI, click **Administration** > **Role Templates**.

2. In the Task Focused UI, from the list of Role Templates, click the name of the role you want to delete.

Click .

3. In the Standard UI, you can delete a role from either the **Role Templates** list page or from the detail page of the role.

- From the **Role Templates** page:
 - a. From the list on the **Role Templates** tab, select the check box next to each role you want to delete.
 - b. Click **Delete**.
- From the detail page of the selected role:
 - a. Click the name of the role you want to delete from the list on the **Role Templates** tab to open its detail page.

- b. On the **Role Information** tab, click **Delete**.

Assigning and revoking roles

An administrator of a parent domain group can assign or revoke roles only from its child groups and users.

For example, an administrator who has the **Assign Roles** administrator permission on a top-level a domain group could assign any role template to users and groups on that business entity or its child sub-entities.

If an administrator assigns a role template to a user or group on a security domain, the same access control that is granted on the corresponding business entity will be propagated to its child entities.

When an administrator assigns a role to a user or group on a lower-level domain that gives the user Read access to a lower-level business entity, the application provides the necessary access to navigate to that lower-level entity even though the user may not have Read access to all of its parent entities.

Example

You have a business entity with the following hierarchical structure:

Company ABC > North America > Boston

The business entity has the following processes:

Company ABC > North America > Boston > P1

Company ABC > North America > Boston > P2

If the administrator of the Boston office assigns a "Process Owner" role to user "Mary" granting Read access only to Processes associated with the Boston entity, then user "Mary" can navigate to processes associated with the Boston entity only, even though "Mary" cannot view the details of the entities Company ABC, North America and Boston.

Assigning and removing a role from a user or group (Task Focused UI)

After role templates are created, you can assign one or more roles to groups and users on a security context point within a business entity security domain.

About this task

If your organization has many security context points, you can filter on the name of a security context point to reduce the scope of the items listed.

You can assign a role to a user or group. Alternatively for users, you can assign roles from the user account. For more information, see [“Modifying user accounts” on page 86](#).

When you revoke a role from a user or group, the role assignment is explicitly removed from the user or group on a given entity.

Disassociating users from a security domain group does not result in removal of their role assignments on that entity.

You can revoke a role assignment from a user or group from the **Role Assignments** tab of the business entity security domain group page. Alternatively for a user, you can remove roles from the user account. For more information, see [“Modifying user accounts” on page 86](#).

Procedure

1. Click  > **Users and Security** > **Domains & Groups**.
2. Click **Domains**.
3. Click the name of the security domain group to which you want to add a role assignment for a user.
4. On the selected security domain group, go to the **Role Assignments** section.

5. Click **Add**.
6. In **User/Group**, find and select each group or user that you want to add.
7. In **Role Type**, select a security point. If only one security point (such as Business Entity) is defined for your system, this is the only value in the list.
8. Select a **Role Template**.
9. Click **Choose** next to **Security Domain**.
 - a) A list of security points is displayed. Expand the folder if needed.
 - b) Select one or more security context points from the list.
 - c) Click **Done**.
10. Click **Add**.
11. To remove a role assignment, go to the **Role Assignments** section. Select the user/group with a check mark and click **Remove**.

Viewing roles assigned to users or groups

You can use several methods to view which roles are assigned to users and groups.

- Run reports
- Open a user account and view role assignments. For more information, see [“Modifying user accounts” on page 86](#).
- Open a user or group and view a list of role assignments.
- Open a business entity security domain group and view a list of role assignments (described below).

Note: Role templates that were assigned directly to a parent or child business entity security domain group can only be viewed from the detail page of that parent or child. Role assignments that are made on a security domain are only displayed for that domain.

In the case of an extended security context model, for example, SOXBusEntity/SOXProcess or SOXBusEntity/SOXProcess/SOXSubprocess security models, role assignments on processes and subprocesses that are associated with the current security domain are also displayed. For more information, see [“Set the system security model” on page 635](#).

Procedure

1. Click  > **Users and Security > Domains & Groups**.
Or, in the Standard UI, click **Administration > Users, Groups and Domains**.
2. Click **Domains**.
3. Click the name of the business entity security domain group whose role assignments you want to view.
4. Go to the **Role Assignments** section.

Adding a role template (Standard UI)

You can add a role template to define application permissions.

The Role Template wizard guides you through creating a new role, selecting object types for inclusion or exclusion, and setting security on the selected object types.

Role template names are not localizable.

Note: Users who have roles that are assigned to a context security point within the Business Entity level only have only navigation access to the parent Business Entity. If users require the ability to view or modify the details of a parent Business Entity, then you must use an entity-based role template to grant explicit Read and/or Write permission to users at an entity security point.

Procedure

1. Ensure that System Admin Mode is disabled.
2. Click **Administration > Role Templates**.
3. On the **Role Templates** tab, click **Add** to open the Add Role Template wizard.
4. On the **Specify Role Details** page:
 - a) In the **Name** box, type a name for the role. For example, Tester01.
 - b) In the **Description** box, optionally type a brief description of this role.
 - c) Click the **Role Type** arrow, and select the type of security context point you want from the list.

Note: If only one security context point type (such as Business Entity) is defined for your system, this is the only value in the list. Security context point types are derived from the security model in effect for your installation.
 - d) Click **Next**.
5. On the **Specify Access Controls** page:
 - a) Select the check box next to each object type for which you want to configure folder permissions. For example, if you wanted to configure permissions for Risk and Test objects, you would select *SOXRisk* and *SOXTest*.

Note: To select all object types, select the check box in the **Name** column.
 - b) In the row for each selected object type, select a setting value for each permission (Write, Delete, and Associate). By default, Read is always set to Granted, and all other permissions are set to Unspecified.

For setting details, see [“Role-based access control permissions” on page 111](#).
 - c) Click **Next**.
6. On the **Specify Permissions** page:
 - a) Select the application permissions that you want to assign to this role template. For a description of the various application permissions, see [“Types of application permissions” on page 91](#).
 - b) Click **Finish**. The new role is listed on the **Role Templates** page.
7. To assign the role to a user or group, see [“Assigning a role to a user or group \(Standard UI\)” on page 119](#).

Assigning a role to a user or group (Standard UI)

After role templates are created, you can assign one or more roles to groups and users on a security context point within a business entity security domain.

If your organization has many security context points, you can filter on the name of a security context point to reduce the scope of the items listed.

About this task

You can assign a role to a user or group with the **Assign Roles** wizard. Alternatively for users, you can assign roles from the user account. For more information, see [“Modifying user accounts” on page 86](#).

Procedure

1. Click **Administration > Users, Groups and Domains**.
2. Under the **Security Domains** group, click the name of the security domain group to which you want to add a role assignment for a user.
3. On the detail page of the selected security domain group:
 - a) Go to the **Role Assignments** tab.
 - b) Click **Assign** to display the **Assign Roles** wizard.

4. On the **Select User(s)/Group(s)** page:
 - a) Click **Add**.
 - b) In the selection box, select the check box next to each group or user you want.
Tip: To expand the group/user hierarchy, click the plus (+) sign.
 - c) Click **Next**.
5. On the **Select Role Type and Role(s)** page:
 - a) Click the **Role Type** arrow and select a security point from the list, and then click **Go**. If only one security point (such as Business Entity) is defined for your system, this is the only value in the list.
 - b) In the **Roles** box, select one or more roles from the list.
 - c) When finished, click **Next**.
6. On the **Select Security Domain(s)** page:
 - a) Optionally, in the **Name** box, type a security context point name or portion of a name and then click **Filter**. If the list of security context points is large, the filter reduces the scope of the list by returning only those items that match the text you typed.
 - b) In the **Security Domains** box, select one or more security context points from the list.
 - c) Click **Finish**.

Revoking a role from a user or group (Standard UI)

When you revoke a role from a user or group, the role assignment is explicitly removed from the user or group on a given entity.

Disassociating users from a security domain group does not result in removal of their role assignments on that entity.

About this task

You can revoke a role assignment from a user or group from the **Role Assignments** tab of the business entity security domain group page. Alternatively for a user, you can remove roles from the user account. For more information, see [“Modifying user accounts” on page 86](#).

Procedure

1. Click **Administration > Users, Groups and Domains**.
2. Under the **Security Domains** root group, click the name of the business entity security domain group from which you want to revoke a role.
3. On the detail page of the selected security domain group:
 - a) Go to the **Role Assignments** tab.
 - b) Select the check box next to the name of each group or user you want to revoke.
 - c) Click **Revoke**. The name of the selected group or user is removed from the list.

Security rules

You can create two levels of security by using security rules:

- [“Record level security” on page 121](#) allows administrators to control access to individual objects in a folder.
- [“Field level security” on page 133](#) allows administrators to control access to individual fields within an object.

Security rules do not replace role-based security. Instead, they provide an extra level of security that can work with role-based security.

Consider this example of record level security. A folder contains 10 tasks. The role-based security grants the Read and Write access controls to all users in a certain role. You define a record level security rule to limit the access for one user who is in that role so that this one user has Read access for Task 1 and Task 8 only.

You can extend the example to field level security. Task 1 contains 10 fields. You can define a field level security rule to limit the access for one user in a certain role. This user has Read access for Field 3 and Field 7 only.

You define security rules for individual object types. After you have defined them, they are applied to all system components, including Reporting, FastMap, Triggers, Reporting Periods, and all available views.

A security rule comprises two parts:

- A formula that determines the conditions for granting the access controls.
 - The formula can be based on these field values: Actor fields, Enumerated fields, Text fields, Date fields, Numeric fields, and Currency fields.
 - The formula can be based on a user who is a member of particular user group or profile.
 - Complex formulae can be based on associations between objects.

For example, a loss event is owned by the business unit where it occurred and is also shared with other business units that are impacted by the loss event. Selected users of the other business units should see its details.
 - The formula can support complex expressions that use terms such as AND, OR, NOT, and nested parentheses.
- The access controls that specify the object access permissions or field access permissions.
 - A record level security rule can specify Create, Read, Update, Associate, and Delete access to object instances.
 - A field level security rule can specify Read only, and Read and Update access to non-system fields within an object.

A security rule formula has the following restrictions:

- They do not support computed text fields.
- They do not support long string fields.
- They do not support NULL values.

The NOT operator does not return objects that have an empty, blank, or null value in the selected field criteria.

- They do not support encrypted simple string or long string data type fields.
- When you use a Multi-Valued User/Group Selector in a security rule, the user or group that you specify in the formula must already exist in your environment.

Note: Security rules are not applied to administrators. They have full permissions for all objects and fields.

Record level security

You can use record level security to control access to individual objects in a folder.

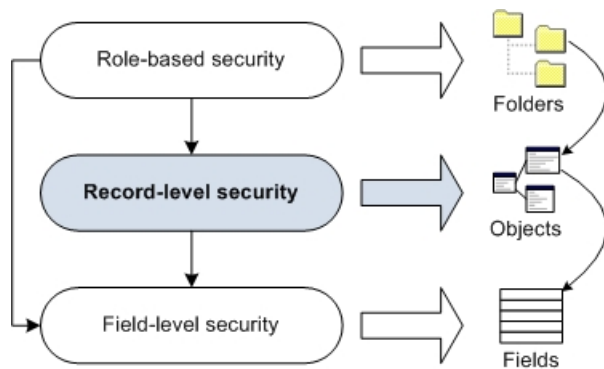


Figure 9. Record level security applies to objects

If no record level security is defined for an object, only role-based security is applied to the object.

When you define a record level security rule, the way that access is restricted depends upon whether the outcome of the formula is true or false when it is applied to an object:

- True: Access to the object is granted, and you can restrict or extend the existing role-based security for that object.
- False: Access to the object is not granted, and role-based security is applied.

When users view an object, they can see associated child objects only under the following circumstances:

- The associated child objects are included in a role template.
- The associated child objects are not included in a role template, but a record level security rule that extends role-based security is applied to the parent object.

RESTRICT and EXTEND rules

When you define a record level security formula, you define RESTRICT rules and EXTEND rules.

A RESTRICT rule is applied after role-based security (RBS). A RESTRICT rule further restricts access to an object. The following formula illustrates how a RESTRICT rule is evaluated:

```
If (RBS=True AND RESTRICT_RULE_RESULT=True), then grant access
```

Notice the AND operator. Role-based security must grant access, and the result of the RESTRICT rule must be true. The result is that users get access to the object if role-based security grants them access and the RESTRICT rule result is also true.

For example, suppose role-based security grants all users in the Finance group READ and UPDATE access on Control objects. But, you want users to be able to do an UPDATE only if they are also the owner of the control object. In this case, you can add a RESTRICT rule on UPDATE that checks the END_USER against the owner field of the object.

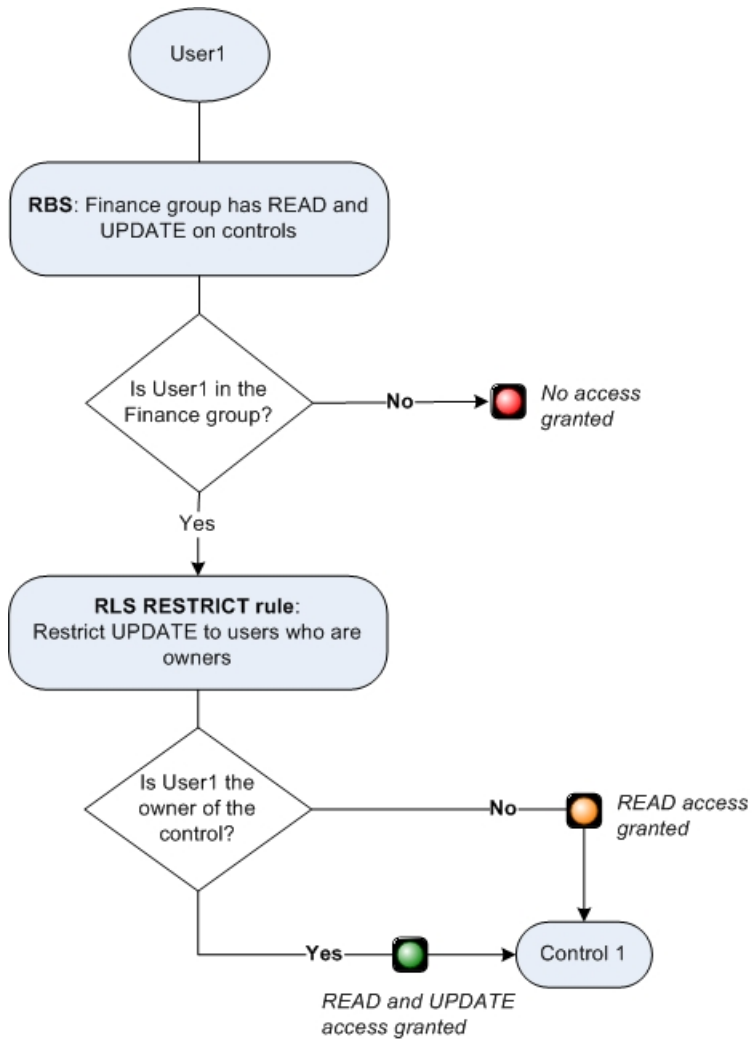


Figure 10. A RESTRICT rule grants UPDATE access if users are in the Finance group and are owners of the control

For a more detailed example, see the record level security scenarios, such as [“Scenario: Objects that are shared across GRC domains”](#) on page 129.

An EXTEND rule is applied in addition to role-based security. An EXTEND rule grants access to an object for which role-based security does not grant access. The following formula illustrates how an EXTEND rule is evaluated:

```
If (RBS=True OR EXTEND_RULE_RESULT=True), then grant access
```

Notice the OR operator. Either role-based security must give access or the EXTEND rule result must be true. The result is that users get access to the object if role-based security gives them access or if the EXTEND rule result is true. Which means users gain access to the object in all of the following scenarios:

- Role-based security is granted and the EXTEND rule result is true, OR
- Role-based security is granted and the EXTEND rule result is false, OR
- Role-based security is not granted and the EXTEND rule result is true.

For example, suppose role-based security grants all users in the Finance group READ and UPDATE access on Control objects. However, you also want users to be able to READ and UPDATE if they are the owner of the control object, regardless of whether they belong to the Finance group. In this case, you can add an EXTEND rule on READ and UPDATE that checks the END_USER against the owner field of the object.

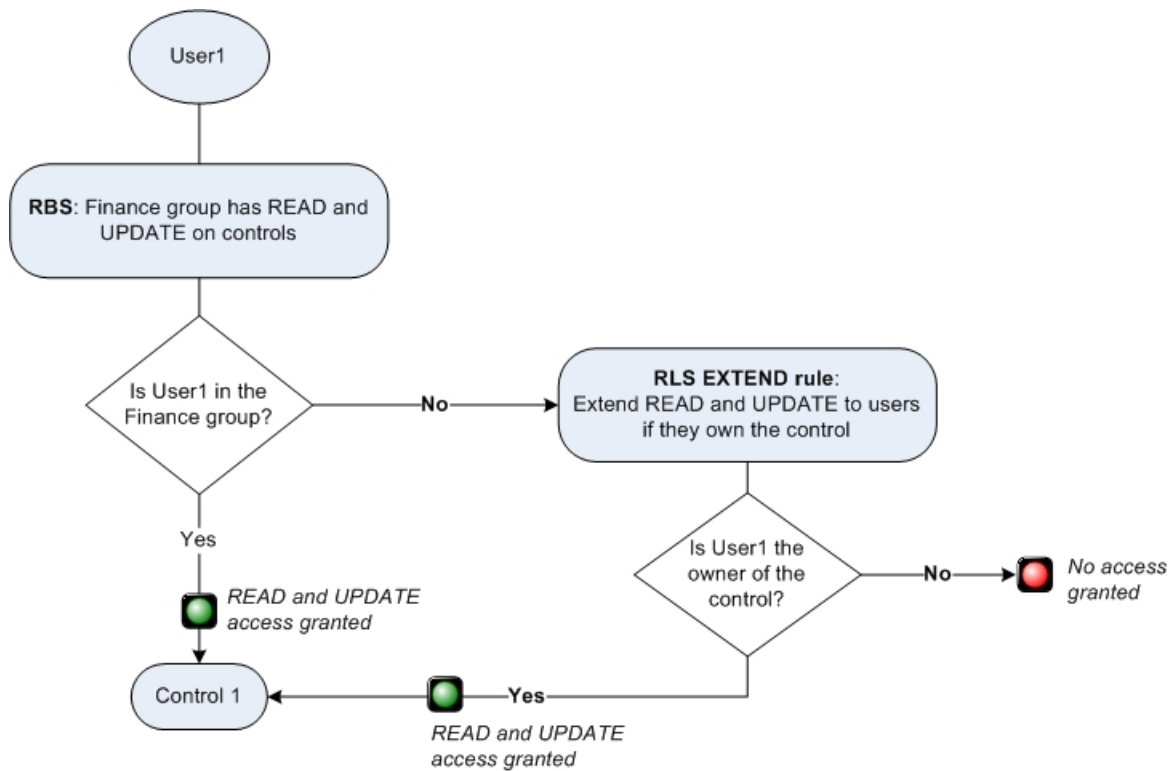


Figure 11. An EXTEND rule grants access to users who are owners of a control, regardless of their group membership

For a more detailed example, see the record level security scenarios, such as [“Scenario: Access for business administrators”](#) on page 133.

Whether you are using a RESTRICT rule or an EXTEND rule, the rule is evaluated within the context of role-based security.

Multiple security rules

You can use multiple RESTRICT and EXTEND rules. Before you combine rules, ensure that you understand how security rules work in combination with each other. Incorrect assumptions about the behavior of security rules can lead to insecure models.

Combining RESTRICT rules

When you have multiple rules on the same object type with the same access, the rules are combined by using an OR expression.

Here is an example of two RESTRICT rules combined:

```

Restrict Rule 1 - Grants READ
Restrict Rule 2 - Grants READ and UPDATE
  
```

Since each rule grants READ access, the two rules are combined whenever the READ access for a user needs to be determined. Each rule is evaluated on its own within the context of role-based security and access is granted if either of the rules evaluates to true. The means that the formula for this example is evaluated in the following manner:

```

If ((RBS=True AND RESTRICT_RULE_1_RESULT=True) OR
(RBS=True AND RESTRICT_RULE_2_RESULT=True)), then grant access
  
```

The result is that a user gets READ access in the following scenarios:

- Role-based security is granted and the RESTRICT rule 1 result is true, OR
- Role-based security is granted and the RESTRICT rule 2 result is true.

Combining **RESTRICT** and **EXTEND** rules

You can combine **RESTRICT** rules with **EXTEND** rules. Each rule is evaluated within the context of role-based security, and then an OR condition is applied. However, do not combine **RESTRICT** and **EXTEND** rules on the same object for the same privilege.

For example, you can combine a **RESTRICT** rule for **READ** and **UPDATE** with an **EXTEND** rule for **DELETE**:

```
Restrict Rule on READ, UPDATE  
Extend Rule on DELETE
```

The rules are evaluated in the following manner:

If evaluating **READ** access:

```
If ((RBS=True AND RESTRICT_RULE_RESULT=True), then grant access
```

If evaluating **UPDATE** access:

```
If ((RBS=True AND RESTRICT_RULE_RESULT=True), then grant access
```

If evaluating **DELETE** access:

```
If (RBS=True OR EXTEND_RULE_RESULT=True)), then grant access
```



Attention: Do not use the same access privilege in both rules. This can lead to results that might not be in-line with the behavior that you expect.

Here is an example of combined **RESTRICT** and **EXTEND** rules to help illustrate the point:

```
Restrict Rule on READ  
Extend Rule on READ
```

The formula is evaluated in the following manner:

```
If ((RBS=True AND RESTRICT_RULE_RESULT=True) OR  
(RBS=True OR EXTEND_RULE_RESULT=True)), then grant access
```

The result is that a user gets **READ** access in all of the following scenarios:

- Role-based security is granted and the **RESTRICT** rule result is true, OR
- Role-based security is granted and the **EXTEND** rule result is true, OR
- Role-based security is granted and the **EXTEND** rule result is false, OR
- Role-based security is not granted and the **EXTEND** rule result is true.

In other words, the user will have **READ** access with role-based security.

How combined security rules are evaluated

It is important to understand how **RESTRICT** rules and **EXTEND** rules are combined.

Many administrators assume that the **EXTEND** rule is evaluated after the **RESTRICT** rule, like this:

```
If ((RBS=True AND RESTRICT_RULE_RESULT=True) OR  
EXTEND_RULE_RESULT=True), then grant access
```

The result would be that a user gets access in the following scenarios:

- Role-based security is granted and the **RESTRICT** rule result is true, OR
- The **EXTEND** rule result is true.

But this is not the case. Each rule is evaluated within the context of role-based security, and then an OR condition is applied:

Let's expand on this example to more clearly see the potential misunderstanding. Suppose that you have a user with the following set of circumstances:

- Role-based security access is granted to the user
- The RESTRICT rule for this user evaluates to FALSE
- The EXTEND rule for this user evaluates to FALSE

Using the formula from the assumed behavior the result of this scenario would be False:

```
((RBS=True AND RESTRICT_RULE_RESULT=True) OR EXTEND_RULE_RESULT=True) =
((True=True AND False=True) OR False=True) =
((True AND False) OR False) =
(False OR False) =
(False)
```

However, the formula that is actually being used is:

```
(RBS=True AND RESTRICT_RULE_RESULT=True) OR (RBS=True OR EXTEND_RULE_RESULT=True) =
(True=True AND False=True) OR (True=True OR False=True) =
(True AND False) OR (True OR False) =
(False OR True) =
(True)
```

Therefore, access would be granted for this user.

It is critical to understand how security rules work in combination with each other before you design your security framework. Incorrect assumptions on behavior can lead to insecure models.

Defining record level security rules

Use record level security rules to control access to individual objects in a folder.

Before you begin

You must enable System Admin Mode before you can define record level security. For more information, see [“Enabling and disabling System Admin Mode” on page 71](#).

Review the following information: [“Best practices for security rules” on page 143](#)

Procedure

1. Click  > **Users and Security** > **Security Rules**.

Or, in the Standard UI, click **Administration** > **Security Rules**.

2. Click the name of the object type for which you want to define a security rule.
3. In the **Record Level Security Rules** section, click **Add**.
4. Add a name and description for the security rule.
5. In the **Security** property, specify how the security rule is combined with role-based security.

- Select **Restrict** to apply both the role-based security and the security rule.

This option configures more restricted security. For example, if role-based security is set to **Read** and the security rule is set to **Update**, the **Restrict** setting provides read only access.

- Select **Extend** to bypass role-based security when the outcome of the formula is true.

For example, if the role-based security is set to **Read** and the security rule is set to **Update**, the **Extend** setting allows a user to update information.

6. Specify the access controls.

For more information, see [“Minimum access controls for object operations” on page 128](#).

Note: Security rules for **Create** access are defined separately from rules for **Read**, **Update**, **Delete**, and **Associate** access. When you click **Create**, the other access options are unavailable.

Create

Users can create objects.

When a rule allows users to create objects, the formula cannot include fields within the object. It can include fields from the parent hierarchy, and other conditions that do not include fields. If you select **Create**, you cannot select any other access control for the rule.

Note: When you define record level security rules for the **Create** access control, use them only to further restrict role-based security.

You must use the **Intended Parent** term in the field when you use **Create**.

Read

Users can view the object.

Update

Users can modify the object.

Delete

Users can delete the object.

Associate

Users can define associations or disassociations between objects.

When a rule allows users to associate objects, the formula cannot include fields within the target of the association. It can include fields from the child hierarchy, and other conditions that do not include fields.

7. Add the formula for the security rule.

You can type the formula or use **Add Path**, **Add Field**, and **Add Terms** to define parts of the formula. You can also use a combination of them. For more information, see [“Grammar for security rules” on page 139](#). (In the Standard UI, the button names are **Path**, **Field**, and **Terms**.)

a) To reference another object, either a parent or child, complete the following actions.

For more information, see [“Paths for parent and child objects” on page 136](#).

- i) Click **Add Path**.
- ii) Click **Parent or Child** and select whether the path follows parent objects or child objects.
- iii) Click **Starting Object Type** and select the object type that is the starting point for the path.
- iv) Click **Ending Object Type** and select the object type that is the ending point for the path.
- v) Click **Search** to view the possible paths.
- vi) Select one or more paths. If you select more than one path, use **Combine Paths** to specify how to use the multiple paths. Select **Any Path** if you want to use any of the paths or select **All Paths** if you want all paths to be used for the rule to be applied.
- vii) Click **Insert**.

b) To define a field condition, complete the following actions.

For more information, see [“Terms for data types” on page 137](#).

- i) Click **Add Field**.
- ii) Select an object type.
- iii) Select the field that you want to use.
- iv) Select an operator. The list of operators changes depending on the field data type.
- v) Enter the value of the field condition.
- vi) Click **Insert** to add the field condition into the rule formula.

If you type the field condition, ensure that you use system names. If you do not specify an object type, the rule uses the object type for the object to which the rule applies. If you specify an object type, the object type must be either the subject of the rule or be specified in a path expression that contains the field reference.

You can use square brackets to ensure that when elements of field references contain spaces or other special characters, these field references are parsed.

c) To add operators or keywords, click **Add Terms**.

8. Click **Validate**.

For more information, see [“Validating a formula for a security rule” on page 142](#).

9. To enable or disable the security rule, click **Status**.

For more information, see [“Enabling or disabling a security rule” on page 142](#).

10. Click **Add**.

Or, in the Standard UI, click **Save**.

Minimum access controls for object operations

Users can perform the following operations on objects: Create, Read, Update, Associate and Delete. Each of these operations requires certain minimum access controls.

Create operation

The following table shows the minimum access controls that a user requires to create an object. Access controls are required for both the parent object and the child object.

Some access controls must be defined by using role-based security rather than record level security (as indicated in the table). In these instances, the access control for the parent object can be defined by using either type of security, but for the child object, it must be defined by using role-based security.

Table 59. Access controls required to create an object				
	Read	Write	Delete	Associate
Parent	Yes			Yes
Child	Yes (from role-based security)	Yes (from role-based security)		Yes (from role-based security)

Read operation

The following table shows the minimum access controls that a user requires to read an object.

These access controls can be defined in the role-based security or the record level security.

Table 60. Access controls required to read an object				
	Read	Write	Delete	Associate
Object	Yes			

Update operation

The following table shows the minimum access controls that a user requires to update an object.

These access controls can be defined in the role-based security or the record level security.

Table 61. Access controls required to update an object				
	Read	Write	Delete	Associate
Object	Yes	Yes		

Associate operation

The following table shows the minimum access controls that a user requires to associate an object. Access controls are required for both the parent object and the child object.

Some access controls must be defined that use role-based security rather than record level security (as indicated in the table). In these instances, the access control for the parent object can be defined by using either type of security, but for the child object, it must be defined by using role-based security.

<i>Table 62. Access controls required to associate an object</i>				
	Read	Write	Delete	Associate
Parent	Yes			Yes
Child	Yes (from role-based security)			Yes (from role-based security)

Delete operation

The following table shows the minimum access controls that a user requires to delete an object. Access controls are required for both the parent object and the child object.

These access controls can be defined in the role-based security or the record level security.

<i>Table 63. Access controls required to delete an object</i>				
	Read	Write	Delete	Associate
Parent	Yes			Yes
Child	Yes		Yes	Yes

The following table shows the minimum access controls that a user requires to delete an object type that is self-contained or recursive, such as a Business Entity or Sub-Process. Access controls are required for both the parent object and the child object.

Some access controls must be defined using role-based security rather than record level security (as indicated in the table). In these instances, the access control for the parent object can be defined using either type of security, but for the child object, it must be defined using role-based security.

<i>Table 64. Access controls to delete a self-contained object</i>				
	Read	Write	Delete	Associate
Parent	Yes			Yes
Child	Yes (from role-based security)		Yes (from role-based security)	Yes (from role-based security)

Scenario: Objects that are shared across GRC domains

Your company implemented the financial management and operational risk solutions. Because the teams that use these solutions share a common organizational hierarchy, they share some common object instances, such as processes. But they do not want to share other object instances, such as risks and controls.

Role-based security means that all users in the financial management and operational risk teams have access to all objects and object instances in the folder. Access controls need to be set for each domain so that users work with only the objects that they are responsible for. As well as securing objects, you are improving usability for your users.

For example, both of the financial management and operational risk teams use the Control object type but they use different instances of the Control object type. You want to enable users in the operational risk team to be able to update their instances of the Control object type. You also want to prevent users in the financial management team from viewing the instances that belong to the operational risk team.

You have two user groups for financial management and operational risk. Role-based security is already defined to grant **Read** and **Write** access controls to all users in the two teams. For example, a user in the SOXUsers group can update the controls that belong to the operational risk team.

Table 65. Permissions for each user group in the scenario			
Domain	User Group	Permitted to work with	Not allowed to work with
Financial Management	SOXUsers	Compliance Controls	Operational Controls
Operational Risk	ORMUsers	Operational Controls	Compliance Controls

To satisfy the security requirements for these two user groups, role-based security is not changed. You add a security rule that further restricts the security that you already defined for the folder.

You define a security rule on the Control object type with the following information:

The formula is:

```
[SOXControl].[OPSS-Ctl].[Domain] IN ('Financial Management') AND END_USER IN
GROUP('SOXUsers')
OR
[SOXControl].[OPSS-Ctl].[Domain] IN ('Operational Risk') AND END_USER IN
GROUP('ORMUsers')
```

When the Security property is set to **Restrict**, both role-based security and the security rule are applied, and the Access controls are set to **Read** and **Update**.

Procedure

1. Click  > **Users and Security** > **Security Rules**.
Or, in the Standard UI, click **Administration** > **Security Rules**.
2. Click the **Control** object type.
3. In the **Record Level Security Rules** section, click **Add**.
4. Add a name and description for the security rule.
5. In the **Security** property, select **Restrict** to have role-based security and the security rule both apply. **Restrict** prevents Compliance users from being able to view or work with the Operational Control.
6. Select the **Read** and **Update** access control check boxes.
7. Add the formula:
 - Click **Add Field** and select the **Control (SOXControl)** object.
 - Select the **Domain** field, and then select the Financial Management domain for the compliance team.
 - Click **Insert**.
 - Click **Add Terms** and select AND, then END_USER, and then IN GROUP.
 - Type 'SOXUsers'.

```
[SOXControl].[OPSS-Ctl].[Domain] IN ('Financial Management')
AND END_USER IN GROUP('SOXUsers')
```

 - Repeat for the Operational Risk domain.
8. Click **Add**.
Or, in the Standard UI, click **Save**.

Scenario: Access to Issue Action Items

Issues that are created under one business unit can cause action items to be assigned to other lines of business. You need to ensure that all action item owners, regardless of business unit, can view the related issue.

An issue can have multiple action items that resolve the issue. The action items can be assigned to different business units and each business unit needs access to the issue object.

In this example, the compliance team has an Issue object that has two action items. One action item is for the compliance team. The other action item is for another business unit to complete some systems work.

Role-based security is set for the compliance team. They have access to all the objects in the folder, including the Issue object. A security rule is not required for the compliance team.

The other business unit needs access to the Issue object that is associated to the action item that they are responsible for. If you add the other business unit to role-based security, the other business unit has access to all objects in the folder. A security rule extends access to the other business unit for their action item and prevents them from working with other objects in the folder.

You define a security rule for the Issue object type with the following information:

The formula is:

```
FOR (Any Child [SOXIssue]/[SOXTask] : [SOXTask].[OPSS-AI].[Assignee] =  
END_USER)
```

When the Security property is set to **Extend**, security is extended beyond role-based security. Users in the other business unit who are the owner of an action item that is associated with this issue can view the issue; however, they cannot view other issues that do not meet the criteria in the formula. The access controls are set to **Read**.

Procedure

1. Click  > **Users and Security** > **Security Rules**.

Or, in the Standard UI, click **Administration** > **Security Rules**.

2. Click the **Issue** object type.
3. In the **Record Level Security Rules** section, click **Add**.
4. Add a name and description for the security rule.
5. In the **Security** property, select **Extend** to have the security rule extend the security that is set on the folder.
6. Select the **Read** access control.
7. Use **Add Path**, **Add Field**, and **Add Terms** to define the formula.
8. Click **Add**.
9. Click the **Task** object type.
10. In the **Record Level Security Rules** section, click **Add**.
11. Add a name and description for the security rule.
12. In the **Security** property, select **Extend** to have the security rule extend the security that is set on the folder.
13. Select the **Read** and **Update** access controls.
14. Use **Add Path**, **Add Field**, and **Add Terms** to define the formula.
15. Click **Add**.

Or, in the Standard UI, click **Save**.

Scenario: Security by job function

All auditors on the same team have the same profile, role template, and security context points. However, each auditor can have a different function for each audit. As an administrator, you want more flexibility in the way you apply security at the field level for each auditor.

This scenario is a variant of the scenario called *Lifecycle security*.

An auditor can have a different job function on different audits. For example, in Audit A, Jim is the lead auditor and can edit more fields than the other auditors.

Table 66. Audit A scenario		
Auditors	Job function	Permissions
Jim	Lead (In-charge)	Jim can edit the Audit A instance of the Audit object and its descendants, Audit Sections, and Audit Workpapers. Jim's access controls are Create, Read, Update, and Associate.
Susan	Field	Susan can read and update specific areas of the Audit Sections and Audit Workpapers in the Audit A instance. Susan's access controls are Read and Update for these areas.
Ellen	Field	Ellen can read and update specific areas of the Audit Sections and Audit Workpapers in the Audit A instance. Ellen's access controls are Read and Update for these areas.

However, in Audit B, Susan is the lead auditor while Jim is a field auditor.

Table 67. Audit B scenario		
Auditors	Job function	Permissions
Susan	Lead (In-charge)	Susan can edit the Audit B instance of the Audit object and its descendants, Audit Sections, and Audit Workpapers. Susan's access controls are Create, Read, Update, and Associate.
Jim	Field	Jim can read and update specific areas of the Audit Sections and Audit Workpapers in the Audit B instance. Jim's access controls are Read and Update for these areas.
Ellen	Not involved in this audit	Ellen has no access controls set for her.

Scenario: Access for business administrators

Some users or groups need access to objects in a different way than most other users and groups in your organization. For example, business administrators need more access controls compared to other users, such as being able to update or delete an object.

This scenario is a variant of [“Scenario: Objects that are shared across GRC domains”](#) on page 129.

Exception management

One example is exception or waiver management.

In general, exceptions from a requirement, control, or process are granted on a project basis. The project is a child of a business entity and is implemented as a risk entity. The project can have secondary associations to a process, a subprocess, or a requirement. Exceptions are child objects of the project and define the requirement, control, or process from which the exception is seeking relief. The project is granted the exception. If no specific project is involved in the exception, the business entity is granted the exception.

All users can create exceptions but they can view only the exceptions that they created. The exception process custodians in IT have the job of reviewing and approving exceptions. You must extend role-based security to grant the exception process custodians in IT the ability to read and update all exceptions.

Privacy incidents

Another example involves the employees who are responsible for privacy incidents.

Specific individuals across the enterprise have responsibility for entering and maintaining information about Privacy incidents. In addition to other access that they have, they are designated as Privacy users and they might be in a Privacy Group or a Privacy Profile. The Privacy users can see all privacy incidents regardless of where the Privacy users are in the business hierarchy. They have access to additional fields on privacy incidents.

Similar functionality can be provided on other object types, such as audit findings, incidents, and waivers.

Scenario: All users can view objects and some users can update objects

Objects can be stored in a common area and shared across GRC domains. In this scenario, only a few users are allowed to update the objects. All other users have read access only.

This scenario is a variant of [“Scenario: Objects that are shared across GRC domains”](#) on page 129.

Role-based security is defined for all users to be able to read the objects in the folder. You want a small group to be able to create and another group to be able to update and associate.

Field level security

You can use field level security to control access to individual fields within an object. Field level security is applied to the set of objects that the user is entitled to by either role-based security or record level security rules. If no field level security is defined for an object, security is applied at the object level (if security rules are defined) or at the folder level.

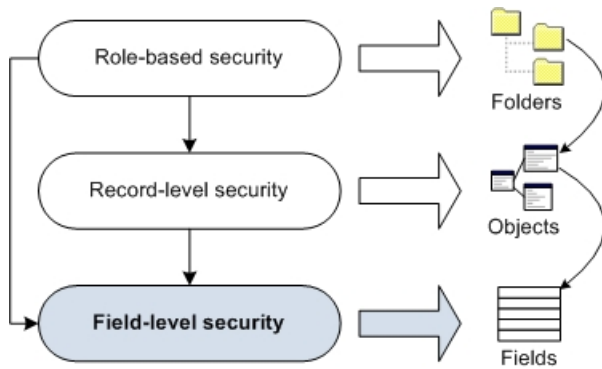


Figure 12. Field level security applies to object fields

When you define a field level security rule, you must consider all the scenarios that are required to access the field. If any scenarios are not defined, a user's access to the field is denied. This is known as redaction.

For example, one rule might specify that if a user is not an Owner, they have only Read access to a field. If a user is an Owner, they have Read and Update access. When the outcome of the formula is true, then Read access or Read and Update access is granted to a user. When the outcome of the formula is false, the field is redacted.

The way that access is restricted depends upon whether the outcome of a formula is true or false when it is applied to a field.

- True: The field is available to users as Read Only or Read and Update.
- False: The field is redacted. Users can see the field label, but not its value. Instead, the value is redacted, and the user sees some text, such as "Confidential" in place of the field value.

Restrictions:

- System fields are not supported.
The system fields are "Name", "Description", "Location", "Creation Date", "Created By", "Last Modification Date", "Last Modified By", and "Comment".
- Computed fields are not supported.
- Simple string fields that are encrypted are not supported.
- If more than one rule applies to a field, the rules are combined by using an OR condition.
- If more than one rule is defined for the same field, and one grants Read access to the field and another grants Read and Update access, then a user is granted Read and Update access if the outcome of the formula for each rule is true.
- Do not include fields that use field level security in Global Search. It might result in users being able to derive data values they otherwise would not have access to.

Redacted fields

When you define a field level security rule, if the outcome of the formula is false, the field is redacted. Users can see the field label, but not its value. Instead, the value is redacted, and the user sees some text, such as "Confidential" in place of the field value.

You can change the label of the text that is used to obscure the field value. For more information, see [“Localizing application text” on page 564](#).

Defining field level security rules

Use field level security to restrict access to specific fields within an object.

Before you begin

You must enable System Administration Mode before you can define field level security.

Procedure

1. Click  > **Users and Security** > **Security Rules**.

Or, in the Standard UI, click **Administration** > **Security Rules**.

2. Click the name of the object type for which you want to define a security rule.
3. In the **Field Level Security Rules** section, click **Add**.
4. Add a name and description for the security rule.
5. Click **Choose Fields**, and select the fields on which to apply the security rule.
6. For each field that you selected, specify the access controls.

Read Only

Users can read the field values, but not update them.

Read and Update

Users can read and update the field values.

7. Add the formula for the security rule.

You can type the formula or use **Add Path**, **Add Field**, and **Add Terms** to define parts of the formula. You can also use a combination of them. For more information, see [“Grammar for security rules” on page 139](#). (In the Standard UI, the button names are **Path**, **Field**, and **Terms**.)

- a) To reference another object, either a parent or child, complete the following actions.
For more information, see [“Paths for parent and child objects” on page 136](#).
 - i) Click **Add Path**.
 - ii) Click **Parent or Child** and select whether the path follows parent objects or child objects.
 - iii) Click **Starting Object Type** and select the object type that is the starting point for the path.
 - iv) Click **Ending Object Type** and select the object type that is the ending point for the path.
 - v) Click **Search** to view the possible paths.
 - vi) Select one or more paths. If you select more than one path, use **Combine Paths** to specify how to use the multiple paths. Select **Any Path** if you want to use any of the paths or select **All Paths** if you want all paths to be used for the rule to be applied.
 - vii) Click **Insert**.
- b) To define a field condition, complete the following actions.
For more information, see [“Terms for data types” on page 137](#).
 - i) Click **Add Field**.
 - ii) Select an object type.
 - iii) Select the field that you want to use.
 - iv) Select an operator. The list of operators changes depending on the field data type.
 - v) Enter the value of the field condition.
 - vi) Click **Insert** to add the field condition into the rule formula.

If you type the field condition, ensure that you use system names. If you do not specify an object type, the rule uses the object type for the object to which the rule applies. If you specify an object type, the object type must be either the subject of the rule or be specified in a path expression that contains the field reference.

You can use square brackets to ensure that when elements of field references contain spaces or other special characters, these field references are parsed.

c) To add operators or keywords, click **Add Terms**.

8. Click **Add**.

Or, in the Standard UI, click **Save**.

Paths for parent and child objects

There can be several paths between objects. For example, there might be two paths between Object A and Object D: A-B-D and A-C-D. When you define a security rule, you specify the starting point (Object A) and the end point (Object B) of the path. You then choose from a list of available paths.

To help you understand parent objects and child objects, consider the metaphor of a school. The students in the entire school can be thought of as having the role of any child. A classroom has a teacher, who can be thought of as the primary parent. The students in this classroom are the primary children of the teacher. Other teachers have the role of any parent. If you want to use the path from a teacher to the students in the teacher's classroom, you use **Primary Parent** or **Primary Child** as the path qualifier.

Parent objects

You can use the following parent objects in the path.

Primary Immediate Parent

Paths follow only to the lowest level primary parent. Use **Primary Immediate Parent** for recursive object types only.

Primary Parent

Paths follow only to the primary parent. There can be only one primary parent.

If a primary parent is specified, the path follows only primary parent relationships.

Any Immediate Parent

Paths follow only to the lowest level parent. Use **Any Immediate Parent** for recursive object types only.

Any Parent

Paths follow to any level of parent, such as grandparent or parent, within recursive object types. For example, a control has a parent that is a subprocess and the subprocess has a parent. When you use **Any Parent** in the path for the control, the parent can be the subprocess or the subprocess's parent.

Child objects

You can use the following child objects in the path.

Primary Immediate Child

Paths follow only to the immediate, highest level child or to the immediate primary child. Use **Primary Immediate Child** for recursive object types only.

Primary Child

Paths follow only to the primary child, which is a child of a primary parent. A primary parent can have several primary children. A child can have only one primary parent.

If a primary child is specified, the path follows only primary child relationships.

Any Immediate Child

Paths follow only to the immediate, highest level children, if the child is a recursive object type. Grandchildren are excluded.

Any Child

Paths follow to any level of child, grandchildren or children, within recursive object types.

Terms for data types

This list contains the data types, operators, keywords, and other terms that are supported in a security rule formula.

The following data types are supported:

- Boolean
- Integer
- Decimal
- Date
- Currency
- Simple string including all display types
- Enumerated (single-valued and multivalued)

Terms that can be used with all data types

The following terms are used with all data types.

AND

Narrows the search for objects. The objects must meet all of the criteria.

OR

Broadens the search for objects. The objects must meet one of the criteria, not all of them.

NOT

Narrows the search by excluding all objects that match the specified criteria.

() (parentheses)

Groups criteria together to show the order in which the rule is applied.

If parentheses are not used, the precedence rules are:

1. **NOT**
2. **AND**
3. **OR**

Terms that are used with numeric data types

The following operators are used with numeric data types, such as decimal, integer, and currency data types. Security rules do not support field criteria on computed text fields or large text fields.

= (equal)

Compares the values in two fields and returns "true" if both contain the same value.

< (less than)

Compares the values in two fields and returns "true" if the second field is less than the first field. The two fields must be of the same data type. For example, both are decimal data types.

> (greater than)

Compares the values in two fields and returns "true" if the second field is greater than the first field. The two fields must be of the same data type. For example, both are decimal data types.

<= (less than or equal)

Compares the values in two fields and returns "true" if the second field is less than or equal to the first field. The two fields must be of the same data type.

>= (greater than or equal)

Compares the values in two fields and returns "true" if the second field is greater than or equal to the first field. The two fields must be of the same data type.

< > (not equal)

Compares the values in two fields and returns "true" if both contain different values.

Uses string variables.

Terms that are used with string data types

The following operators are used with data types that require strings, such as enumerated strings and simple strings. Security rules do not support long strings.

CONTAINS

Determines whether a multiple-select field contains a specific value or set of values.

ENDS WITH

Determines if the field value ends with the specified text.

LIKE

Determines if a field value matches the specified pattern string.

STARTS WITH

Determines if the field value starts with the specified text.

IN

Determines if the field value is in the specified field.

Terms that are used with date data types

TODAY

Returns today's date.

TOMORROW

Returns tomorrow's date.

NOW

Returns the current date and time.

You can specify a date in the future or in the past. For example:

- `NOW(5)` specifies a date five days from now.
- `NOW(2, 'm')` specifies a date two months from now.
- `NOW(-5)` specifies a date five days ago.
- `NOW(-2, 'y')` specifies a date two years ago.

You can use year, month, week, day, hour, minute, or second.

YESTERDAY

Returns yesterday's date.

DATE

Specifies the date and time as a string in the ISO format: `YYYY-MM-DD` and `hh:mm:ss.sTZD`.

You can also specify the date and its format as a string: `DATE('09/05/2013', 'MM/dd/yyyy')`

Terms that are used with other data types

END_USER

Returns the logged-in user.

END_USER_PROFILE

Returns the profile for the logged-in user.

IN GROUP

Returns the user group for the logged-in user.

IN PROFILE

Returns the specified field value that is in the specified profile.

INTENDED PARENT

Tests the parent under which a new object is to be created. It can be used only when you define a **Create** record level security rule.

Use **INTENDED PARENT** when you want to control what a user or group can create. For example, you can allow specific users to create risks for subprocesses but not for issues.

When you use **INTENDED PARENT**, the condition can depend on the object type that is referenced as intended parent. The condition can also depend on the object type of the security rule's subject. A path expression that uses intended parent is considered false if the intended parent is not of the specified object type.

Grammar for security rules

As an administrator, you need to understand the grammar for a security rule formula so that you understand the potential impact of adding a rule.

condition

Condition is the basic building block for a security rule formula.

```
|---+-- predicate -----+--|
+-- NOT -- condition -----+
+--condition -- AND -- condition --+
+--condition -- OR -- condition --+
+-- path-condition -----+
'-- ( -- condition -- ) -----'
```

The following rule applies to condition:

- If parentheses are not used, the precedence rules are:
 1. NOT
 2. AND
 3. OR

path-condition

```
>>-- FOR ( --+-- v----- AND -----,
| v----- path-direction -- path --+-- : -- condition -- ) --<<
| v----- OR -----, |
+--- path-direction -- path --+--
'-- intended-parent -----'
```

predicate

```
|---+-- scalar --+-- = ---+-- scalar ---+--|
|          +-- < ---+          |
|          +-- > ---+          |
|          +-- <= ---+         |
|          +-- >= ---+         |
|          +-- <> ---+         |
+-- like-predicate -----+
+-- starts-with-predicate-----+
+-- contains-predicate-----+
+-- ends-with-predicate-----+
+-- in-predicate -----+
+-- in-group-predicate-----+
'-- in-profile-predicate-----'
```

scalar-value

```
|---+-- field-reference -- +-+|
+-- end-user-profile --+
+-- boolean -----+
+-- integer -----+
+-- decimal -----+
+-- date -----+
+-- currency -----+
+-- simple string -----+
```

```
+-- enum-value -----+
'-- function -----'
```

field-reference

```
>>+-----+-- . -- field-group -- . -- field-name --<<
    '-- object-type --'
```

The following rules apply to the `field-reference`:

- If no object-type is given, the object type is that of the object to which the rule applies.
- If an object-type is given, it must either be the subject of the rule or been specified in a path expression that contains the field-reference.
- All elements of the field reference must be system names.
- Optional square brackets can be used to assure parsing in case elements of field references contain spaces or other special characters.

```
end-user-profile
```

```
|-- END_USER_PROFILE ( --+-- field-reference --+-- ) --|
                        '-- string -----'
```

```
function
```

```
|---+-- TODAY -----+--+|  
+-- TOMORROW -----+--+|  
+-- NOW -----+-----+|  
|      |    .-- ( 0, 'd' ) -----+|  
|      |    |       .-- , -----'d' ---|  
|-- NOW --+-- ( -- offset +-----+--+ ) -+-+|  
                   |-- , ---+'y' ---+  
                       +-+'m' ---+  
                       +-+'d' ---+  
                       +-+'h' ---+  
                       +-+'mi' ---+  
                       '--+'s' ---+
```

like-predicate

```
|-- field-reference -- LIKE -- pattern-string --|
```

The following rule applies to the `like`-predicate:

- The pattern string must be a string constant.
- For information on what is supported for the `like`-predicate, see [“Limitations on special characters in filters for long string fields”](#) on page 269 and [“Using complex logic in a search filter \(Standard UI\)”](#) on page 274.

starts-with-predicate

```
|-- field-reference -- STARTS WITH -- string --|
```

contains-predicate

```
|-- field-reference -- ENDS WITH -- string --|
```

ends-with-predicate

```
|-- field-reference -- ENDS WITH -- string --|
```

in-predicate

```
|-- scalar-value -- IN --+-- scalar-value -----+--|
      |               v---, -----|
      |-- ( --- scalar-value --+-- ) --|
```

The following rules apply to in-predicate:

- If a single field reference is given, it must be a multivalued field.
- If multivalued fields are used in the list, they are unnested.

in-group-predicate

```
|-- scalar-value -- IN GROUP --+-- scalar-value -----+--|
      |               v---, -----|
      |-- ( --- scalar-value --+-- ) --|
```

The following rules apply to in-group-predicate:

- If a single field reference is given, it must be a multivalued field.
- If multivalued fields are used in the list, they are unnested.

in-profile-predicate

```
|-- scalar-value -- IN PROFILE --+-- string -----+--|
      |               v---, -----|
      |-- ( --- string --+-- ) --+|
```

The following rules apply to in-profile-predicate:

- If a single field reference is given, it must be a multivalued field.
- If multivalued fields are used in the list, they are unnested.

path

```
      v-----
|-- object-type ----- / -- object-type --+--|
```

path-direction

```
      .-- ANY -----
|--+-- PRIMARY --+-----+-- CHILD ---
      | IMMEDIATE --|      PARENT --+--|
```

intended-parent

```
|-- INTENDED PARENT OF TYPE -- object-type -- |
```

Rules

- Combining multiple paths with AND or OR is semantically equivalent to specifying multiple path expressions with the same condition combined by AND or OR.

- For combined paths, the end point of all paths in the path expression must have the same object type. The condition can contain references only to the shared starting points and ending points as well as any references to outer paths that lead up to the subject.
- A path expression for a given path of object types is considered true if the condition is true for any instantiation of the path.
- Except for combined paths described earlier, the condition can depend on any object type along the path of the path-expression.
- The condition may also depend on object types along the path of containing path-expressions or the subject object type of the rule.
- When using `intended-parent`, the condition can depend on the object-type referenced as intended parent as well as the subject object-type of the rule. A path expression that uses the intended parent clause is considered false if the intended parent is not of the specified object-type or the operation is not Associate or Create.
- Depending on the path-direction specified, the path lists a connected series of object types relative to the current context either following parent or child relationships.
- The outermost path must start with the rule's subject type. Nested paths must start with the endpoint of the immediately containing path.
- If IMMEDIATE is specified and the end point of the path is a recursive object type, the path stops at the bottom most parent of that type or the top most child.
- If PRIMARY is specified, the path will follow only primary parent relationships.

Enabling or disabling a security rule

You can work on a security rule without making it available to your users. When the security rule is ready, you can enable it. Conversely, you can withdraw a security rule by disabling it so that you can make all required changes to it.

Before you begin

You must enable System Admin Mode before you can work with security rules. For more information, see [“Enabling and disabling System Admin Mode”](#) on page 71.

Procedure

1. Click  > **Users and Security** > **Security Rules**.
Or, in the Standard UI, click **Administration** > **Security Rules**.
2. Select the object type that contains the security rule that you want to enable or disable.
3. Click the check box of the rule, and then click **Enable** or **Disable**.
Or, in the Standard UI, click **Enable** or **Disable** in the **Actions** column.

Validating a formula for a security rule

When you validate a formula for a security rule, IBM OpenPages with Watson checks the completeness of the formula that you entered and verifies that the syntax of the rule is correct.

Note: The validation is validating only whether the rule is syntactically correct. It does not validate whether the values are valid. The values that you provide are validated when you save.

For example, in the following expression, the left side of the equation shows an enumerated string field. The right side has a Boolean value. The syntax would be correct if the status field was Boolean. The validation does not recognize that the data types are different.

```
[SOXIssue].[OPSS-Iss].[Status] = FALSE
```


Before you begin

You must enable System Admin Mode before you can work with security rules. For more information, see [“Enabling and disabling System Admin Mode” on page 71](#).

Procedure

1. Click  > **Users and Security** > **Security Rules**.
Or, in the Standard UI, click **Administration** > **Security Rules**.
2. Select the object type that contains the security rule that you want to validate.
3. Click the name of the security rule.
Or, in the Standard UI, click the security rule and then click **Edit**.
4. Click **Validate** for the formula that you want to validate.
5. When you see a message that the formula has successfully validated, click **Done**.
Or, in the Standard UI, click **Save**.

Deleting a security rule

When a security rule is no longer required, you can delete it. You cannot undo the deletion.

Before you begin

You must enable System Admin Mode before you can work with security rules. For more information, see [“Enabling and disabling System Admin Mode” on page 71](#).

Procedure

1. Click  > **Users and Security** > **Security Rules**.
Or, in the Standard UI, click **Administration** > **Security Rules**.
2. Select the object type that contains the security rule that you want to delete.
3. Click the check box of the rule, and then click **Delete**.
Or, in the Standard UI, click **Delete** in the **Actions** column.

Best practices for security rules

When you configure security rules, consider the following best practices.

Creating rules for file attachments

You can create rules that extend or restrict access to file attachments. The object type for file attachments is SOXDocument. However, the SOXDocument object type is also used by system files, such as FastMap templates. When you create a rule on SOXDocument, you need to ensure that users can still access the system files.

For example, suppose that users in the Policy group need access to file attachments where the document type is Policy Attachment. But you also need to ensure that all users can access the FastMap export template. You need to create a formula with two clauses: one to grant all users access to the FastMap template and another to grant the Policy group access to the file attachments they need.

```
[SOXDocument].[System Fields].[Location] STARTS WITH '/Templates/FastMap/%'  
OR ([SOXDocument].[OPSS-File].[Document Type] IN ('Policy Attachment'))  
AND END_USER IN GROUP ('Policy'))
```

Combining record level security rules for an object type

If you have a (Create) and (Read or Associate) rule for an object type, you must add an extra OR condition to the (Read or Associate) rule. This condition is required so that the (Create) and (Read or Associate) rules can work together.

The OR condition looks like this:

```
(NOT(FOR (Any Parent [Rule_ObjectType]/PATH : 1=1))
AND [Rule_ObjectType].[System Fields].[Created By] = END_USER)
```

Where:

- Rule_ObjectType is the object type in which the Read rule is created.
- PATH is the path of the Read rule, starting from the Rule_ObjectType.

The following example shows the security rule for LossEvent to control the Read operation for LossEvents under BusinessEntity.

```
OR (NOT(FOR (Any Parent [LossEvent]/[SOXBusEntity] : 1=1))
AND [LossEvent].[System Fields].[Created By] = END_USER)
```

Lifecycles

You can use security rules with lifecycle triggers.

Security rules are evaluated before lifecycle triggers and actions modify an object. If an object's state before the lifecycle trigger meets the record level security criteria, you can update the object. The lifecycle trigger might modify fields so that the object state no longer meets the record level security rules.

If you use lifecycle triggers, consider using workflows or calculations instead. For more information, see [Chapter 15, “Configuring GRC Workflow,” on page 495](#) and [Chapter 14, “Configuring GRC Calculations,” on page 457](#).

Custom security for projects

You can set custom security access control (Read, Write, Delete, Associate) on folders for Project Milestones and Project Action Items.

Note: The custom security feature is deprecated. Use role based security instead. For more information, see [“Role-based security model” on page 105](#).

Use the **Custom Security** task to set custom security access control. By default, inheritance for access control (ACL) is set to true.

The **Custom Security** task is available in both the Task Focused UI and the Standard UI. Changes made in one user interface are immediately reflected in the other.

By default, the custom ACL shows only Project Milestone and Project Action Items. To show other object types in the custom ACL, add values to the **Common > Custom ACL Object Types** setting in the **Settings** page. Add object names separated by commas.

About the folder hierarchy and inheritance

On the Access Control page, the Milestone folder is the container for Project Milestone objects and the Task folder is the container for Project Action Item objects. Both of these folders are under a Plan folder.

By default, inheritance on the Plan folder is set to false and cannot be changed. Inheritance on the Milestone and Task object folders, by default, is set to true. You can disable inheritance on these folders. If a folder does not have an ACL set for a particular group, the application looks back up the folder tree until it finds an ACL for that group and uses it for the current folder. When folder inheritance is enabled

and a folder does not have an ACL set for a particular group, the application looks backwards up the folder tree until it finds an ACL for that group and uses it for the current folder.

Creating an Access Control List

You can control which users and groups can access Project Milestones and Project Action Items.

Note: The custom security feature is deprecated. Use role based security instead. For more information, see [“Role-based security model”](#) on page 105.

Before you begin

Before you can add an Access Control List (ACL), you must disable System Admin Mode if it is enabled. See [“Enabling and disabling System Admin Mode”](#) on page 71.

Procedure

1. Log on to IBM OpenPages with Watson as a Super Administrator user with the **Access Control Lists** application permission set.

2. Click  > **Users and Security** > **Custom Security**.

Or, in the Standard UI, click **Administration** > **Custom Security**.

3. Expand **Default** > **Plan** and do the following:

- For Project Milestones - click the **Milestone** link.
- For Project Action Items - click the **Task** link.

4. In the **Access Control** section, click **Add Access Control**.

If you are using the Standard UI, click **Actions** > **Add**.

5. On the access control page:

- a) Search for the user or group you want to add.
- b) For each permission (Read, Write, Delete, Associate), select a setting value (Granted, Inherited, Denied).
- c) Click **Add**.

Note: Read permission is required for Write and Associate access, and Write access is required in order for Delete access to be granted. You can select any combination of permissions, but when you save the ACL, it will be modified to be a valid combination of permissions.

Editing an Access Control List

You can edit an Access Control List for a user or group.

Before you begin

Before you can edit an Access Control List (ACL), you must disable System Admin Mode if it is enabled. See [“Enabling and disabling System Admin Mode”](#) on page 71.

Procedure

1. Log on to IBM OpenPages with Watson as a Super Administrator user with the **Access Control Lists** application permission set.

2. Click  > **Users and Security** > **Custom Security**.

Or, in the Standard UI, click **Administration** > **Custom Security**.

3. Expand the folder hierarchy and click the folder that has the Access Control List that you want to modify.

4. In the **Access Control** section:

- a) Click the user or group for which you want to modify access control.
- b) Make the necessary changes.
- c) Click **Save**.

If you are using the Standard UI, click **Actions** > **Save**.

Deleting an Access Control List

You can delete an Access Control List for a user or group.

Before you begin

Before you can delete an Access Control List (ACL), you must disable System Admin Mode if it is enabled. See [“Enabling and disabling System Admin Mode” on page 71](#).

Procedure

1. Log on to IBM OpenPages with Watson as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click  > **Users and Security** > **Custom Security**.
Or, in the Standard UI, click **Administration** > **Custom Security**.
3. Expand the folder hierarchy and click the folder that has the Access Control List that you want to modify.
4. In the **Access Control** section:
 - a) Click  next to the user or group for which you want to delete access control and click **Delete**.
If you are using the Standard UI, click the user or group and click **Actions** > **Remove**.

Encryption

IBM OpenPages with Watson supports the following optional features:

- You can configure a custom encryption key to encrypt passwords that are stored in OpenPages properties files.
If you do not configure a custom encryption key, the passwords in properties files are still encrypted. However, your organization policies might require you to use a custom encryption key.
- You can encrypt specific fields in the IBM OpenPages with Watson repository to prevent system administrators from viewing confidential data directly from the database.

Create a keystore

You can create a keystore for IBM OpenPages with Watson.

Create the encryption keystore file and key pair

Before you can set up the encryption keystore in IBM OpenPages with Watson, you must create an encryption keystore file that contains the key pair details.

The file must use the Java format (jceks). Although you can use any keytool to create the file, it must use the same format as a Java keystore.

The encryption key must use one of the following encryption algorithms. Any other algorithms are not supported.

Table 68. Supported encryption algorithms

Algorithm name	Key size
3DES	168
AES128	128
AES192	192
AES256	256

When you run the `keytool -genseckey` command, you are prompted for the keystore password and the key password.

Important: You must use the same password for the keystore and the key.

In the following example, the command generates a keystore that uses the supported Java format (jceks). The encryption key uses a 3DES encryption algorithm with a key size of 168.

```
keytool -genseckey -alias openpages -keyalg 3DES -keysize 168
-storetype jceks -keystore keystore-3DES.jks
```

In the following example, the command generates a keystore that uses the supported Java format (jceks). The encryption key uses an AES encryption algorithm with a key size of 256.

```
keytool -genseckey -alias openpages -keyalg AES -keysize 256
-storetype jceks -keystore keystore-AES256.jks
```

Setting up the encryption keystore

The encryption keystore is a file that stores the key that you use to encrypt passwords that are stored in properties files and to encrypt data in the IBM OpenPages with Watson repository.

Before you begin

You need a keystore file and you need to know the keystore password. For more information, see [“Create the encryption keystore file and key pair” on page 146](#).

Procedure

1. Enable System Admin Mode.
For more information, see [“Enabling and disabling System Admin Mode” on page 71](#).
2. Click  > **Users and Security** > **Encryption Keystore**.
Or, in the Standard UI, click **Administration** > **Encryption Keystore**.
3. Click **Edit**.
4. Enter the name of the encryption key in the **Key Name** field.
5. Enter the alias in the **Key Alias** field.

Important: Ensure the alias that you specify is an exact match to the alias in the keystore file.

6. Enter the keystore location in the **Keystore Location** field.

For security reasons, you cannot browse to the location, you must type it manually.

7. Select the encryption algorithm that is used by the key in the **Algorithm** field.
8. Enter the keystore password in the **Keystore Password** field,

Important: Ensure the password that you specify here is an exact match to the password in the keystore file.

9. Confirm the password in the **Re-enter Keystore Password** field.
10. Enter a description for the keystore in the **Description** field.

11. Click **Update**.

Note: If you change any of these keystore properties in future, you must update the keystore. For more information, see [“Updating the encryption keystore” on page 153](#).

Configure a custom encryption key for passwords in properties files

You can configure a custom encryption key to encrypt the passwords that are stored in properties files.

Note: If you already configured a custom key but the properties of the key changed, see [“Updating the encryption keystore” on page 153](#).

You need to do the following tasks to use a custom key to encrypt passwords that are stored in property files:

- Create a file that contains the encryption keystore and key pair. See [“Create the encryption keystore file and key pair” on page 146](#).
- Set up the encryption keystore. [“Setting up the encryption keystore” on page 147](#)
- Create a `keystore.properties` file. See [“The keystore.properties file” on page 148](#).
- Update the property files on all application servers to use the custom encryption key. See [“Updating property files on application servers to use a custom key” on page 149](#).
- Update property files on all reporting servers to use the custom encryption key. See [“Updating property files on reporting servers to use a custom key” on page 150](#).
- If you use global search, update property files on the search server to use the custom encryption key. See [“Updating property files on the search server to use a custom key” on page 151](#).

The keystore.properties file

Create a `keystore.properties` file. The file defines the custom encryption key to use for passwords that are stored in IBM OpenPages with Watson properties files.

Do this task after you create a keystore and configure it in IBM OpenPages with Watson.

Use the following text as a template:

```
#Tue December 13 23:35:46 EDT 2018
key.password=<password for the encryption key>
key.alias=<alias (name) of the encryption key>
keystore.path=<full path to the .jks file>
store.password=<password for the keystore>
```

Note: The `key.password` and the `store.password` must be the same.

For the `keystore.path` parameter, use a directory that all of your application servers and reporting servers can access. If you use global search, ensure that your search server can also access the directory. You have the following options:

- Specify a network location that all application servers, reporting servers, and the search server can access.
- Or, store the `.jks` file in the same directory on each server.
- Or, create a `keystore.properties` file for each type of server.

Example:

```
#Tue December 13 23:35:46 EDT 2018
key.password=password
key.alias=openpages
keystore.path=C:\\admin\\keystore-AES128.jks
store.password=password
```

Updating property files on application servers to use a custom key

After you configure a custom encryption key, update the property files on your application servers to use the custom encryption key.

Before you begin

The following tasks must be completed before you begin:

- Create a file that contains the encryption keystore and key pair. See [“Create the encryption keystore file and key pair”](#) on page 146.
- Set up the encryption keystore. [“Setting up the encryption keystore”](#) on page 147
- Create a keystore.properties file. See [“The keystore.properties file”](#) on page 148.
- Verify that all application servers can access the keystore.path that is specified in the keystore.properties file.

Procedure

1. Stop all OpenPages application servers, admin and non-admin.
See [“Stopping application servers”](#) on page 843.
2. Copy the keystore.properties file to the <OP_HOME>/aurora/bin directory.
3. Edit the aurora.properties file.

- a) Go to the <OP_HOME>/aurora/conf directory.
- b) Make a backup copy of the aurora.properties file.
- c) Open the aurora.properties file in a text editor.
- d) Change the following password values after the equal sign to plain text.

```
security.system.password=<openpages_system_password>  
database.PASSWORD=<openpages_db_password>
```

- e) Save and close the file.

When you restart the servers later in this task, the passwords are re-encrypted with the custom encryption key.

4. Edit the aurora_auth.config file.
 - a) Go to the <OP_HOME>/aurora/conf directory.
 - b) Make a backup copy of the aurora_auth.config file.
 - c) Open the aurora_auth.config file in a text editor.
 - d) Locate the security.search.user.credentials parameter
 - e) Change the value after the equal sign to plain text.
 - f) Save and close the file.

When you restart the servers later in this task, the password is re-encrypted with the custom key that you specified.

5. Edit the op-backup-restore.env file.
 - a) Go to the <OP_HOME>/aurora/bin directory.
 - b) Make a backup copy of the op-backup-restore.env file.
 - c) Open the op-backup-restore.env file in a text editor.
 - d) Change the following password values after the equal sign to plain text.
 - IBM Db2: DB_OP_PWD: Type the password of the schema owner for the OpenPages database.
 - Oracle:
 - DB_SYSTEM_PWD: Type the password of the SYSTEM user for the OpenPages database.

- DB_SYS_PWD: Type the password of the DBA user for the OpenPages database.
- DB_OP_PWD: Type the password of the schema owner for the OpenPages database.
- e) Save and close the file.
- 6. Re-encrypt the passwords in the `op-backup-restore.env` file with the custom encryption key that you specified.
 - a) Go to the `<OP_HOME>/aurora/bin` directory.
 - b) Run the following command:

Windows

```
OPBackup.cmd secure
```

Linux

```
./OPBackup.sh secure
```

- c) Open the `op-backup-restore.env` file in a text editor and verify that the passwords are encrypted.
7. If you are using a horizontal cluster, do steps 2-6 on each application server in the cluster.
8. Start all OpenPages application servers, admin and non-admin.
See [“Starting application servers” on page 841](#).

Results

The passwords are encrypted with the custom encryption key that you specified in the `keystore.properties` file.

Updating property files on reporting servers to use a custom key

After you configure a custom encryption key, update the property files on your reporting servers to use the custom encryption key.

Before you begin

The following tasks must be completed before you begin:

- Create a file that contains the encryption keystore and key pair. See [“Create the encryption keystore file and key pair” on page 146](#).
- Set up the encryption keystore. [“Setting up the encryption keystore” on page 147](#)
- Create a `keystore.properties` file. See [“The keystore.properties file” on page 148](#).
- Verify that all reporting servers can access the `keystore.path` that is specified in the `keystore.properties` file.

Procedure

1. Copy the `keystore.properties` file to the `<CC_HOME>/tools/bin/` directory.
2. Edit the `op-cc-backup-restore.env` file.
 - a) Go to the `<OP_HOME>/tools/bin` directory.
 - b) Make a backup copy of the `op-cc-backup-restore.env` file.
 - c) Open the `op-cc-backup-restore.env` file in a text editor.
 - d) Change the following password value after the equal sign to plain text.

```
DB_CC_PWD=<cognos_db_password>
```

- e) Save and close the file.

3. Re-encrypt the passwords in the `op-cc-backup-restore.env` file with the custom encryption key.
 - a) Go to the `<CC_HOME>/tools/bin` directory.
 - b) Run the following command:

Windows

```
OPCCBackup.cmd secure
```

Linux

```
./OPCCBackup.sh secure
```

- c) Open the `op-cc-backup-restore.env` file in a text editor and verify that the password is encrypted.
4. If you are using a horizontal cluster, update each reporting server in the cluster.

Results

The passwords are encrypted with the custom encryption key that you specified in the `keystore.properties` file.

Updating property files on the search server to use a custom key

If you use global search, update the property files on your search server to use the custom encryption key.

Before you begin

The following tasks must be completed before you begin:

- Create a file that contains the encryption keystore and key pair. See [“Create the encryption keystore file and key pair” on page 146](#).
- Set up the encryption keystore. [“Setting up the encryption keystore” on page 147](#)
- Create a `keystore.properties` file. See [“The keystore.properties file” on page 148](#).
- Verify that the search server can access the `keystore.path` that is specified in the `keystore.properties` file.

Procedure

1. Copy the `keystore.properties` file to the `<SEARCH_HOME>` directory.
2. Disable global search and stop the global search services.
See [“Stopping the global search services by using a script” on page 845](#) or [“Stopping the global search services” on page 847](#).
3. Open a shell or command window as an administrator and then go to the `<SEARCH_HOME>` directory.
4. Run the following command to encrypt the password with the custom key:

Tip: You do not need to change the password. You can use the same value for the `<old_op_db_password>` and `<new_op_db_password>` parameters.

```
java -jar opsearchtool.jar setdbuserpassword -username <op_db_username>  
-password <old_op_db_password> -newusername <op_db_username> -newpassword  
<old_op_db_password>
```

You do not need to change the global search service (Apache Solr) password. The global search service password is stored in a registry setting, not in a properties file.

5. Start the global search services.
See [“Starting the global search services by using a script” on page 844](#). Or if you want to start global search as a service, see [“Starting the global search services on Windows” on page 845](#) or [“Starting the global search services on Linux” on page 846](#).

Results

The password that the search server uses to access the database server is encrypted with the custom encryption key that you specified in the `keystore.properties` file.

Configure field level encryption

You can encrypt specific fields in the IBM OpenPages with Watson repository to prevent system administrators from viewing confidential data directly from the database. Data in encrypted fields is shown as a string of random characters.

Simple string and long string field data types are supported.

Fields that are encrypted are not eligible for use in Global Search.

Note: Before encrypting long strings in OpenPages running on Oracle 12.2, refer to the following Technote: <http://www.ibm.com/support/docview.wss?uid=swg22010106>. The Technote describes a potential issue and how to resolve it by obtaining the appropriate patch from Oracle support and applying it to your environment. The IBM OpenPages with Watson reporting framework handles encrypted fields by running a database function to decrypt them. When a long string (CLOB) field is made encrypted, the framework must be regenerated to call this database function. For more information, see [“Generating the reporting framework”](#) on page 974.

Restrictions:

- The maximum size of long strings that can be encrypted is 2 MB.
- Do not include encrypted long string fields in the search criteria for a filter because they can return unexpected results.

You need to do the following tasks to use field level encryption:

- Create a file that contains the encryption keystore and key pair. See [“Create the encryption keystore file and key pair”](#) on page 146.
- Set up the encryption keystore. [“Setting up the encryption keystore”](#) on page 147
- Place the keystore file on the application servers in your environment.

In a horizontal environment, the keystore file must be available to each application server. There are two options:

- Each application server must have access to the file location on the admin application server.
- The file must be available in the same location on each application server.

In a non-clustered environment, place the keystore file on the admin application server.

- Enable the keystore. See [“Enabling the encryption keystore”](#) on page 152.

Note: If you already configured field level encryption but the properties of the key changed, see [“Updating the encryption keystore”](#) on page 153.

Enabling the encryption keystore

After you set up the encryption keystore, you must enable it to encrypt the IBM OpenPages with Watson repository. If required, you can disable the keystore later to decrypt the repository again.

About this task

When you enable the keystore, any fields that are currently marked for encryption are automatically encrypted in the repository. If there are no fields that are marked for encryption, the keystore is enabled, meaning that it is ready to automatically encrypt any fields that are marked for encryption from now. For information on marking fields for encryption, see [“Encrypting field values”](#) on page 209.

Procedure

1. Click  > **Users and Security** > **Encryption Keystore**.
Or, in the Standard UI, click **Administration** > **Encryption Keystore**.
2. Click **Enable**.

Depending on the size of the repository, encryption can take a long time. Encryption runs as background event. You can view the progress by clicking **Refresh**.

Disabling the encryption keystore

After the IBM OpenPages with Watson repository is encrypted, you can disable the keystore to decrypt the repository again.

About this task

When you disable the keystore, any fields that are currently marked for decryption are automatically decrypted in the repository. If no fields are marked for decryption, the keystore is disabled, meaning that it is ready to automatically decrypt any fields that are marked for decryption from now. For information on marking fields for decryption, see [“Decrypting field values” on page 210](#).

Procedure

1. Click  > **Users and Security** > **Encryption Keystore**.
Or, in the Standard UI, click **Administration** > **Encryption Keystore**.
2. Click **Disable**.

Depending on the size of the repository, decryption can take a long time. Decryption runs as background event. You can view the progress by clicking **Refresh**.

Updating the encryption keystore

Your company IT policy might require that you periodically change the encryption key. Whenever the encryption key details change, you must update the encryption keystore in IBM OpenPages with Watson.

Note:

If field level encryption is already enabled, you do not need to disable the encryption keystore to update it.

Procedure

1. Create a new keystore file.
For more information, see [“Create the encryption keystore file and key pair” on page 146](#).
2. Create a keystore.properties file. See [“The keystore.properties file” on page 148](#).
3. Click  > **Users and Security** > **Encryption Keystore**.
Or, in the Standard UI, click **Administration** > **Encryption Keystore**.
4. Click **Edit**.
5. Enter the current encryption keystore password to access it.
6. Update the details of the keystore.
For more information, see [“Setting up the encryption keystore” on page 147](#).
7. Click **Update**.

If you use field level encryption and it is enabled, the fields are re-encrypted using the new encryption key. Depending on the size of the repository, updating the encryption can take a long time. Field encryption runs in the background. You can view the progress by clicking **Refresh**.

8. Update passwords in properties files.

- a) On each application server, change the passwords in properties files to plain text, save the files, and then restart the application server.
For more information, see [“Updating property files on application servers to use a custom key” on page 149.](#)
- b) On each reporting server, change the passwords in properties files to plain text, save the files, and then restart the reporting server.
For more information, see [“Updating property files on reporting servers to use a custom key” on page 150.](#)
- c) If you use global search, change the passwords in properties files to plain text, save the files, and then restart the server.
For more information, see [“Updating property files on the search server to use a custom key” on page 151.](#)

The passwords are encrypted with the updated encryption key when you restart the servers.

9. If you use IBM OpenPages Loss Event Entry, re-enter the password for each locale.

- a) Start the configuration tool. Go to `http://<server_name>:<port>/openpages/app/jspview/lossevent#/editconfig`
- b) Log in with a user account that is a member of the OPAdministrators group.
- c) Under the **Locales** section, expand each locale and enter the password.
- d) Close the configuration tool.

The passwords are encrypted with the updated encryption key.

10. If you use LDAP for user provisioning, do the following steps:

- a) Click  > **Users and Security** > **User LDAP Configuration**.
Or, in the Standard UI, click **Administration** > **User LDAP Configuration**.
- b) Edit the LDAP configuration.
- c) In the **Security credentials** field, re-enter the password that is used to authenticate with the LDAP server.
- d) Click **Save**.

The security credentials are encrypted with the updated encryption key.

11. If you use natural language classifiers, do the following steps:

- a) Click  > **Integrations** > **Mapping and Taxonomy Suggestions**.
Or, in the Standard UI, click **Administration** > **Cognitive Services** > **Natural Language Classifiers**.
- b) Edit the classifier configuration.
 - Natural Language Classifier: In the **API Key** field, re-enter the API key of the Natural Language Classifier instance.
 - Watson Discovery Analyze API: Re-enter the password. (Task Focused UI only)
- c) Click **Save**.
- d) Repeat these steps for each classifier configuration.

The API keys are encrypted with the updated encryption key.

LDAP user authentication

IBM OpenPages with Watson supports the use of an LDAP (Lightweight Directory Access Protocol) authentication server to control user access.

To use LDAP user authentication, you integrate OpenPages with Watson with an LDAP data source.

Only one login module can be active at the same time. OpenPages with Watson supports a single namespace. All users must be authenticated through the same data source. Multiple authentication modules can be used in a multi-forested environment.

Users that are created or imported into OpenPages with Watson must also be defined in the LDAP authentication server. The administrator managing the OpenPages with Watson users is responsible for maintaining the correlation between the OpenPages with Watson user list and the external LDAP data source. If a user is disabled on the OpenPages with Watson server, the user must be manually disabled on the LDAP Directory server.

Note: If an LDAP Directory server is being used for user authentication, the **Change Password** option is disabled in OpenPages with Watson. When an LDAP server is used, passwords are not maintained in OpenPages with Watson. The password must be changed in the LDAP server.

You can also configure OpenPages with Watson to use an external LDAP user authentication server over SSL. For more information, see [“Modifying the LDAP configuration file for LDAP over TLS” on page 802.](#)

Configuring the LDAP Authentication Module

To successfully use an LDAP Directory Server with IBM OpenPages with Watson, you must configure the LDAP Authentication Module to recognize the presence of the LDAP server.

To configure OpenPages with Watson to work with an external LDAP authentication source, complete the following tasks:

- [“Adding existing users to the LDAP server” on page 155](#)
- [“Modifying the LDAP configuration file” on page 155](#)

Adding existing users to the LDAP server

You can add existing IBM OpenPages with Watson users to an LDAP server.

Make sure to refer to your LDAP Directory Server documentation for the steps required to add users to the LDAP server.

Important: If you are using Microsoft Active Directory Users and Computers as your LDAP authentication server, the user name is limited to 20 characters. User names that exceed the 20-characters limit are truncated to 20 characters. This length limitation does not occur in the LDAP server provided by Sun.

All users that require access to the OpenPages with Watson application or server platform must be added to the LDAP authentication server. In addition, the following users will need to be added to the LDAP server:

- OPSsystem

Note: If you specify a password for the OPSsystem account that is different from the one installed by the product, you will need to complete [“Changing the OPSsystem password” on page 773](#) to change the OPSsystem account password system-wide.

- The OpenPages with Watson Super Administrator (for more information, see [“The Super Administrator” on page 75](#))
- OPAdministrator (only if you are using this account)

Modifying the LDAP configuration file

You must modify the authentication configuration file to enable the LDAP Directory Server that you are using.

Note: If you are using LDAP over SSL, see [“Modifying the LDAP configuration file for LDAP over TLS” on page 802.](#)

The `aurora_auth.config` file contains three authentication modules:

- Openpages - the default internal user directory
- OpenpagesIP - a sample LDAP configuration for the Sun One Directory Server
- OpenpagesAD - a sample LDAP configuration for the Microsoft Active Directory Server

The only module that the IBM OpenPages with Watson system pays attention to is the module that is named Openpages. Therefore, you need to make a backup of the Openpages module, rename the OpenpagesIP or OpenpagesAD to Openpages, and then change the settings to reflect the settings of your LDAP server.

Procedure

1. Stop all OpenPages with Watson services.
2. Open and edit the `<OP_Home>/aurora/conf/aurora_auth.config` file in a text editor.

Where:

`<OP_Home>` is the installation location of the OpenPages with Watson application.

3. Find the Openpages module and change its name to OpenpagesDefault.
4. Modify either the OpenpagesIP or OpenpagesAD module name to Openpages.
 - If you are using a Microsoft Active Directory server, change the name of the OpenpagesAD module to Openpages.
 - If you are using a Sun One Directory Server, change the name of the OpenpagesIP module to Openpages.
 - If you are using a different LDAP server, you can use either of these modules. Choose a module to use as a template and change its name to Openpages.
5. Specify the correct values for the following properties in the module that you named Openpages:

provider.url

Change the value to the hostname and port number for the LDAP authentication server. For LDAP, the protocol is `ldap` and the port is the LDAP port number (by default, 389).

base.dn

The top level of the LDAP directory tree structure (Domain Name) on the LDAP server. If the users to be authenticated are located in multiple locations within your Active Directory structure, list all of the locations explicitly by using the distinguished names of the locations, each separated by a semi-colon.

For example:

```
base.dn="DC=LDAPTesting,DC=local;CN=Users,DC=LDAPTesting,DC=local;
OU=Auditors,OU=External Auditors,OU=Staff,DC=LDAPTesting,DC=local"
```

user.attr.id

The attribute name of the user identifier (for example, `uid`, `cn`, etc.)

Additional custom parameters

You can add additional custom parameters that are supported by the Java Naming and Directory Interface (JNDI). Precede a JNDI property with the `ctx.env.` prefix.

For example, if you want to use the JNDI property `com.sun.jndi.ldap.connect.timeout`, use `ctx.env.com.sun.jndi.ldap.connect.timeout=<value>` in the `aurora_auth.config` file.

For information about JNDI properties, see the [Java SE documentation](http://docs.oracle.com/javase/7/docs/technotes/guides/jndi/jndi-ldap.html#JNDIPROPS) (<http://docs.oracle.com/javase/7/docs/technotes/guides/jndi/jndi-ldap.html#JNDIPROPS>).

For example:

```
Openpages
{
    com.openpages.aurora.service.security.namespace.LDAPLoginModule
```

```

        required debug=false
        provider.url="ldap://myserver.company.com:389"
        security.authentication="simple"
        security.search.user.dn="cn=Directory Manager"
        security.search.user.credentials="openpages"
        base.dn="ou=people,o=IBM,c=US"
        user.attr.id="uid"
    ;
};

```

6. When you are finished editing the file, save your changes and exit.
7. Restart all services.

Results

You have configured the OpenPages with Watson system to use an external LDAP user authentication server.

Setting up mixed-mode authentication

Use mixed-mode authentication when not all users can use a single namespace for authentication.

This solution should be used by customers who do not want to create the OPSysSystem, SOXAdministrator, OpenPagesAdministrator, or OPAdministrator user accounts on their LDAP server but do want all their users to be authenticated by LDAP. The following procedure creates a new namespace and modifies user names (such as OPSysSystem) to authenticate against the OpenPages with Watson authentication module rather than LDAP.

Procedure

1. To create the namespace modules in the `aurora_auth.config` file, log on to the application server.
2. Find and open the `aurora_auth.config` file.
3. Create or update the namespace modules in the file as follows:

```

OpenpagesDefault
{
com.openpages.aurora.service.security.namespace.AuroraLoginModule
required debug=false;
};

Openpages
{
com.openpages.aurora.service.security.namespace.LDAPLoginModule required
debug=false
provider.url="ldap://192.168.0.169:30429"
security.authentication="simple"
base.dn="DC=LDAPTesting,DC=local;OU=People,DC=LDAPTesting,DC=local"
user.attr.id="uid"
;
};

```

4. To create the namespace in the database, log into the database instance with the database id, such as OPENPAGES.
5. Run the following SQL to create the OpenpagesDefault namespace:

```

insert into namespaces (NAMESPACEID, NAME, JAASLOGINMODULE,
DESCRIPTION) values (namespaceidseq.nextval, 'Openpages Security',
'OpenpagesDefault', 'Default Openpages Security Namespace');

```

6. Run the following SQL to point an ID to the new namespace:

```

update actors set namespaceid = (select namespaceid from
namespaces where JAASLOGINMODULE = 'OpenpagesDefault') where actorid =
(select actorid from actorinfo where name = 'user_name');

```

For example, the following SQL will have the OPSys use the OpenpagesDefault namespace for authentication:

```
update actors set namespaceid = (select namespaceid from
namespaces where JAASLOGINMODULE = 'OpenpagesDefault') where actorid =
(select actorid from actorinfo where name = 'OPSystem');
```

7. Commit the changes to the database.

Configuring a multi-forested LDAP authentication

IBM OpenPages with Watson supports the use of multiple LDAP authentication servers in a multi-forested configuration. If the application cannot find the user in the first authentication server, it will check the next server in the list and repeat until it finds the user or checks all listed authentication servers.

When listing multiple LDAP servers, the `aurora_auth.config` file must be modified to contain multiple sets of server information.

This file is located in the `<OP_Home>\aurora\conf` directory, where `<OP_Home>` is the installation location of the OpenPages with Watson application. By default, this is `c:\OpenPages`.

This is accomplished by grouping the server information by index key, as in the following example:

```
com.openpages.aurora.service.security.namespace.LDAPLoginModule required
debug=true
provider.url.1="ldap://10.128.22.106:389"
security.authentication.1="simple"
security.search.user.dn.1="CN=Administrator,CN=Users,DC=parent,DC=parentchild,DC=localdomain"
security.search.user.credentials.1="Op3nPag3s"
base.dn.1="DC=parent,DC=parentchild,DC=localdomain"
user.attr.id.1="CN"
provider.url.2="ldap://10.128.22.107:389"
security.authentication.2="simple"
security.search.user.dn.2="CN=Administrator,CN=Users,DC=child,DC=parent,DC=parentchild,DC=localdomain"
security.search.user.credentials.2="Op3nPag3s"
base.dn.2="DC=child,DC=parent,DC=parentchild,DC=localdomain"
user.attr.id.2="CN"
```

By adding a ".1" key to the end of each parameter, OpenPages with Watson can parse the settings correctly and differentiate between separate LDAP server information sets. You would append a ".2" to the keys for the second LDAP server, and so on.

For single LDAP server implementations, you do not need to append an identifier to the end of the parameter names.

Chapter 6. Managing the reporting schema

The IBM OpenPages with Watson application supports the use of a real-time reporting schema model that allows reports to access information as it is entered into the system. Data does not have to be exported to an external reporting database repository.

See [“Changes that require the reporting schema to be updated or recreated” on page 159](#) for a list of tasks that require the reporting schema to be recreated. The OpenPages with Watson application does not have to be restarted after recreating the reporting schema.

You can access the reporting schema using either the Task Focused UI or the Standard UI. Changes made in one interface are immediately reflected in the other.

You can also use a command line tool. For more information, see [“Generating the reporting schema and framework from a command line” on page 164](#).

Changes that require the reporting schema to be updated or recreated

You can update the reporting schema or recreate it when necessary.

Updating the reporting schema

Update the reporting schema in the following cases:

- When you set or change the display type of a field to Multi-Valued User Selector or Multi-Valued Group Selector or Multi-Valued User Group Selector
- When you import a profile by using ObjectManager or the **Import Configuration** feature.

When you update the reporting schema, you do not need to regenerate the reporting framework.

For more information, see [“Updating the reporting schema” on page 162](#).

Recreating the reporting schema

Table 69 on page 159 lists the actions that require the reporting schema to be recreated. In some cases, the reporting framework must also be regenerated.

Table 69. Recreating the reporting schema and regenerating the reporting framework		
This type of change...	Requires this to be regenerated...	
	Reporting schema	Reporting framework
Adding a new field to a field group.	No	Yes
Adding a new object type.	No	Yes
Adding a new association between object types.	No	Yes
Removing object types or attributes. For information, see “Deleting a custom object type” on page 266 .	Yes	Yes
Encrypting a long string (CLOB) field.	No	Yes
Enabling facts or dimensions.	No	Yes
Defining, modifying, or deleting business entity recursive object levels.	No	Yes

Table 69. Recreating the reporting schema and regenerating the reporting framework (continued)

This type of change...	Requires this to be regenerated...	
	Reporting schema	Reporting framework
Removing a field from a field group.	No	Yes
Disabling an association between object types.	No	Yes
Disabling facts or dimensions.	No	Yes
Switching the security model. Note: Switching the security model after data is loaded or migrated into the system is not recommended and requires assistance from the OpenPages Professional Services team.	Yes	Yes
Changing the value of the Populate past periods setting. For information, see “Populating past reporting periods” on page 160 .	Yes	No
Changing any setting used to compose URL links in the reporting schema, for example, the Host, Port, and Protocol settings. For information about updating the reporting schema, see “Updating URL host pointers for reports” on page 769 if you want to run the RPS_Update SQL script or “Creating or recreating the reporting schema (Task Focused UI)” on page 162 if you are update manually.	Yes	No
Adding an index to an RT_column by using the Settings > Platform > Reporting Schema > Create Index on Fields setting.	Yes	No
Configuring the triangles setting. For information, see “Triangle object relationships” on page 955 .	Yes	No

Other situations that require the reporting schema to be created, recreated, enabled, and disabled are described in the *IBM OpenPages with Watson Installation and Deployment Guide*.

For more information, see [“Creating or recreating the reporting schema \(Task Focused UI\)” on page 162](#) or [“Creating or recreating the reporting schema \(Standard UI\)” on page 163](#). It is a good idea to schedule this activity ahead of time, since creating a reporting schema requires that the application be in System Admin Mode. In this mode, users are not able to log onto the system and users who are currently logged in are not able to commit changes to the repository.

Note: Depending on your changes, recreating the reporting schema and regenerating the reporting framework for Cognos reports might not cause your modifications to appear in the standard reports. You might also need to modify the your existing reports or create new reports to display the additional information (such as adding new fields).

Populating past reporting periods

You can control whether data from previous reporting periods or the current reporting period is included in the reporting schema.

Use the following procedure to change the **Populate Past Periods** setting, which controls what is populated in the reporting schema. By default, the reporting schema is populated with the data from previous reporting periods.

Procedure

1. Click  > **System Configuration** > **Settings**.
2. Expand the **Platform | Reporting Schema** folder hierarchy.
3. Click the **Populate Past Periods** setting to open its details page.
4. In the **Value** field, type one of the following values:

Table 70. Past period reporting values	
Value	Description
true	The reporting schema is populated with the data from previous reporting periods. This value is set by default. Note: When this setting is set to true, it increases the amount of data that is published by the Reporting Schema operation and increases the time it takes to drop and recreate the Reporting Schema.
false	The reporting schema is populated with the data from the current reporting period.

5. Click **Done**.

What to do next

Recreate the reporting schema (see, [“Changes that require the reporting schema to be updated or recreated” on page 159](#)).

Reporting schema permissions

Before performing any actions on a reporting schema, you must have specific application permissions set on your account.

The Reporting Schema task is used to control the creation and deletion of the reporting schema. Administrative-level users who have the Reporting Schema application permission can access the task.

For more information, see [“Types of application permissions” on page 91](#)).

Table 71. Reporting schema and framework permissions	
This application permission...	Is used to...
Reporting Schema	• Access the  > System Configuration > Reporting Schema menu item in the Task Focused UI. • Access the Administration > Reporting Schema menu item in the Standard UI.
System Administration Mode	Enable and disable System Admin Mode.

Creating or recreating the reporting schema (Task Focused UI)

You can create, recreate, enable and disable a reporting schema. You can also drop reporting schema tables to reclaim database space.

Before you begin

The system must be in System Administration Mode (see [“Enabling and disabling System Admin Mode”](#) on page 71) to modify the reporting schema.

Check the setting that controls whether past reporting periods are included in the reporting schema. For more information, see [“Populating past reporting periods”](#) on page 160.

About this task

Creating a new reporting schema automatically enables the reporting schema, while dropping the reporting schema automatically disables it.

When the reporting schema is enabled, the database tracks changes to the application data and allows the reporting engine to access the updated data. When the schema is disabled, the database no longer tracks changes to the application data, but is still aware of changes to the schema (such as new fields).

The system keeps a log of each reporting schema operation that has been performed.

Procedure

1. Click  > **System Configuration** > **Reporting Schema**.
2. To create or recreate a reporting schema, perform one of the following actions:
 - If a reporting schema already exists, click **Re-Create** to drop the existing schema and create a new schema.
 - If no reporting schema exists, click **Create**. The new reporting schema is automatically enabled.
3. To enable the reporting schema, click **Enable**.
4. To disable the reporting schema, click **Disable**.
5. To reclaim the database space taken by the reporting schema tables, click **Drop**. This automatically disables the reporting schema.

What to do next

To view details of a reporting schema operation and review errors, use search to find the operation you want to view. A summary page opens with two tabs, **Information** and **Log**.

When the creation task (or re-creation task) is complete, update the Reporting Framework so that the Cognos reports can access the new schema. For more information, see [“Updating the reporting framework \(Task Focused UI\)”](#) on page 977.

Updating the reporting schema

Update the reporting schema.

Procedure

1. Log in to OpenPages as a user with administrative privileges.
2. Enable System Admin Mode (SAM). Click , and then click **Enable System Admin Mode**.
3. Click  > **System Configuration** > **Reporting Schema**.
4. Click **Update**.

5. Click **Refresh** until the process is 100% complete.
6. Disable SAM. Click , and then click **Disable System Admin Mode**.

Accessing the reporting schema (Standard UI)

You can create, recreate, disable, drop, and view the status of a reporting schema from the Reporting Schema detail page.

Before you begin

The system must be in System Admin Mode (see [“Enabling and disabling System Admin Mode”](#) on page 71) to modify the reporting schema.

About this task

Complete the following steps to access the reporting schema:

Procedure

1. Log on to the IBM OpenPages with Watson Standard UI interface as a user with the **Reporting Schema** application permission set.
2. From the menu bar, select **Administration** and click **Reporting Schema**.

Creating or recreating the reporting schema (Standard UI)

You can create or recreate the reporting schema.

Before you begin

Complete the following steps to create or recreate a reporting schema:

Procedure

1. Access the Reporting Schema. Log on to the IBM OpenPages with Watson application user interface as a user with the **Reporting Schema** application permission set.
 - a) From the menu bar, select **Administration** and click **Reporting Schema**.
2. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode”](#) on page 71.
3. Perform one of the following actions:
 - If a reporting schema already exists, click **Re-Create** to drop the existing schema and create a new schema.
 - If no reporting schema exists, click **Create**.
4. When the creation task (or re-creation task) is complete, update the Reporting Framework so that the Cognos reports can access the new schema. For more information, see [“Updating the reporting framework \(Standard UI\)”](#) on page 978.

Enabling and disabling the reporting schema (Standard UI)

Creating a new reporting schema automatically enables the reporting schema, while dropping the reporting schema automatically disables it.

When the reporting schema is enabled, the database tracks changes to the application data and allows the reporting engine to access the updated data. When the schema is disabled, the database no longer tracks changes to the application data, but is still aware of changes to the schema (such as new fields).

Note: You must be in System Admin Mode (SAM) to enable the icons that allow you to perform these tasks.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71](#).
2. From the menu bar, select **Administration** and click **Reporting Schema**.
3. Enable or disable the reporting schema:
 - Click **Enable** to enable the reporting schema. If the schema does not exist, click the **Create** icon to create the reporting schema. Creating the reporting schema will automatically enable the new schema.
 - Click **Disable** to disable the reporting schema. If you want to reclaim the database space taken by the reporting schema tables, you must click the **Drop** icon. This will automatically disable the reporting schema.

Viewing reporting schema operation details (Standard UI)

IBM OpenPages with Watson keeps a log of each reporting schema operation that has been performed.

Before you begin

Complete the following steps to view the reporting schema details:

Procedure

1. Access the Reporting Schema. Log on to the IBM OpenPages with Watson application user interface as a user with the **Reporting Schema** application permission set.
 - a) From the menu bar, select **Administration** and click **Reporting Schema**.
2. On the **Reporting Schema Operations** pane, click the name of the operation.
3. On the **Operation Detail** pane, click **View Log**.

Generating the reporting schema and framework from a command line

You can generate the reporting schema and the reporting framework by using the `RpsRpf.sh | .cmd` tool from a command line.

Before you begin

- JAVA_HOME must be set.
- The client tools must be installed. For more information, see [“Installing tools and utilities \(IBM OpenPages with Watson\)” on page 824](#) or [“Installing tools and utilities in Cloud Pak for Data” on page 44](#).

About this task

You can use the `RpsRpf.sh | .cmd` tool to create the reporting schema, the reporting framework, or both. When you generate the reporting framework, all framework models are generated.

You must have the following application permissions:

- To create or re-create the reporting schema, you must be a super administrator. Or, you must have these permissions:
 - **Administration > System Administration Mode**

- **SOX > Administration > Reporting Schema**
- To generate the reporting framework, you must be a super administrator. Or, you must have this permission:
- **SOX > Administration > Reporting Framework**

Procedure

1. Go to the directory where client tools are installed:

IBM OpenPages with Watson

Go to the `<OP_HOME>/bin` directory on the application server.

Or, if you installed the client tools on a remote system, go to the `openpages-tools-client/bin` directory. The computer must be able to communicate with the OpenPages application server.

IBM OpenPages for IBM Cloud Pak for Data

Go to the `openpages-tools/bin` directory on the remote system where you installed the client tools package. The remote system must have access to IBM OpenPages for IBM Cloud Pak for Data.

2. Verify the properties in the `openpages-tools-client.properties` file.

IBM OpenPages with Watson

Verify that `rest.url.path` is set to the base URL of the public REST API on the application server, for example: `https\://<host>\:<port>/grc/api`

IBM OpenPages for IBM Cloud Pak for Data

- Verify that `rest.url.path` is set to the base URL of the public REST API, for example `https\://<cpd_url>/openpages-<instance_name>-grc`

Replace `<cpd_url>` with the URL of IBM Cloud Pak for Data. Replace `<instance_name>` with the name of the OpenPages instance.

- Verify that `platform.cloudpak.jwt.auth` is set to `true`.

3. Open the `RpsRpf.properties` file.

4. Set credentials in the properties file

IBM OpenPages with Watson

```
OPENPAGES_ADMIN_USERNAME=
OPENPAGES_ADMIN_PASSWORD=
```

IBM OpenPages for IBM Cloud Pak for Data

```
OPENPAGES_JWT_USER=
OPENPAGES_JWT_TOKEN_OR_API_KEY=
```

5. Set the following parameters:

RPSRPF_ACTION_TYPE

- RPS: Create the reporting schema.
- RPF: Generate the reporting framework.
- BOTH: Create the reporting schema, and then generate the reporting framework.

DROP_REPORTING_SCHEMA

Optional. If you want to drop the reporting schema and re-create it, change `DROP_REPORTING_SCHEMA` to `true`.

Note: Do not modify `RPF_PARAMS`.

The following example shows a properties file for IBM OpenPages with Watson. With this configuration, the tool creates the reporting schema and then generates the reporting framework.

```
# OpenPages Administrator account
OPENPAGES_ADMIN_USERNAME=OpenPagesAdministrator
OPENPAGES_ADMIN_PASSWORD=
#JWT Auth
OPENPAGES_JWT_USER=
OPENPAGES_JWT_TOKEN_OR_API_KEY=
# Action type
# RPS - Reporting Schema Creation
# RPF - Reporting Framework Generation
# BOTH - Both RPS and RPF ( default )
RPSRPF_ACTION_TYPE=both

# Comma-separated reporting Framework options. Default is all options for v6 schema
RPF_PARAMS=dimensionFacts,customQuerySubjects,genType_6,i18NTranslationType_6
# Uncomment the next line for V5 Reporting Framework
#RPF_PARAMS=dimensionFacts,customQuerySubjects,genType_552,i18NTranslationType_552

# Drop reporting schema when it creates one
DROP_REPORTING_SCHEMA=false
```

Note: The V5 Reporting Framework is no longer supported. Do not uncomment the V5 Reporting Framework line.

6. Run the `RpsRpf.sh` | `.cmd` tool:

Windows

Open a command prompt as an administrator, and then run the following command:

```
RpsRpf.cmd
```

Linux

Run the following command:

```
./RpsRpf.sh
```

Note: If a framework generation process is already in progress, the script returns information about the process.

7. Check the log file for errors and warnings: `<client_tools>/logs/openpages-tools-client.log`

Where `<client_tools>` is the directory that you used in step “1” on [page 165](#).

Chapter 7. Managing reports

The IBM OpenPages with Watson application contains a set of reports that allows users with the correct permissions to quickly view and organize information about the current state of your, for example, financial, compliance, or operational project. For example, users can quickly view information grouped by either user, by location, or view.

Use the **Manage Pages and Templates** task on the Administration menu in the Task Focused UI to define report pages and page templates.

In the **Manage Pages and Templates** task, the **Add Folder**, **Add Page**, and **Add Page Template** options are displayed if a folder is selected with a check mark. The **Copy**, **Move**, and **Delete** options are displayed if multiple folders or one or more report pages or page templates are selected with a check mark.

Supplied reports

The OpenPages with Watson application comes with a selection of predefined and supplied reports that allow you to quickly view important information about your project.

Note: The list of reports in this documentation is for a fresh installation of the OpenPages with Watson application. If you have additional reports tailored to your particular business needs or have upgraded from an earlier version of the application, the classification of the supplied reports may differ from the classification documented here.

OpenPages with Watson V6 folder reports

The V6 folder in IBM OpenPages with Watson contains subfolders for the report types that are available. The All Documentation report resides at the top level of the reporting hierarchy.

Important: In reference to Reporting Framework V6, V6 refers to the latest framework version, not to any specific OpenPages with Watson release number.

Table 72. OpenPages with Watson V6 folder reports and folders	
Report or folder name	Description
All Documentation report	Detailed view of an organization's entity hierarchy, associated internal controls documentation, and counts of related issues, files, and links in the current reporting period. This is filtered by business entity. There are detailed subreports for each count.
Administrative Reports folder	Folder that contains predefined administrative reports such as a list of files that are checked out.
Audit Reports folder	Folder that contains predefined audit reports such as an audit summary.
Issue Reports folder	Folder that contains predefined reports on issues such as the issues and associated action items for a chosen reporting period and business entity.

Administrative Reports folder

OpenPages with Watson includes the following, predefined administrative reports:

Table 73. Administrative Reports folder

Report Name	Description
Checked Out Files	Listing of attached Files in a checked out state in the current reporting period. You can sort by: • Name of File. • Full Path of the folder where the File is stored. • User who has checked out the File. • Date the File was checked out.
Disassociated Objects	Listing of objects that do not have associated parent objects in the current reporting period. You can filter for specific object types and can sort by: • Name of object. • Full Path of the folder where the object is stored.

Audit Reports folder

In addition to the reports listed in the following table, the Audit Reports folder contains the following subfolders:

- Configuration (see [Table 76 on page 169](#))
- Security (see [Table 77 on page 170](#))

Table 74. Audit Reports folder

Report Name	Description
Audit Change	Lists all object changes that fulfill the user's runtime filtering criteria. Users can filter the report on Business Entity, Start Time, End Time, specific object type, and status. For an explanation of audit events and the values in the Status and Item columns of the report, see "Description of Audit Change events and values" on page 168.
Audit Summary	Administrative summary of changes to documentation data, which is filtered by date and time range. You can also filter by Business Entity and object type and drill into a detailed Audit subreport.

Description of Audit Change events and values

An audit event is a combination of an action and object aspect (that is, the object, a relationship, or attribute of the object) that was affected by the event. The Audit Change report identifies change events for any field value change.

Notice: This information also applies to the detail subreport from the Audit Summary report.

To understand the nature of each audit event, it is useful to understand how objects are created, associated, and shared.

In the hierarchy of objects in the system, a child object (such as a Control) might be associated to more than one parent object (such as a Risk). Conversely, any one parent object (such as a Risk) might have several associations to different child objects (such as Controls). These associations or relationships are flagged as either *Primary* or *Non-Primary*.

Any one parent object (such as a Risk) might have multiple child objects (such as Controls). However, the system allows only one of the object parent-child relationships to be marked as "Primary". Primary

associations are used to determine the path that the system should follow when you are executing a number of operations that require object hierarchy traversal.

In the OpenPages with Watson application, the following operations traverse the Primary Association path:

- SCOR rule execution
- Cascade Delete (including those requested by SCOR delete rules)
- Sign-offs, Locking, and Un-Locking
- Hierarchical copy and move

Audit Trail Reports are "parent object centric" when the report captures events that pertain to an object associations. For an object, all association-related events are defined as those where the object acts as a parent. Events where the object acts as a child are reported in context of the corresponding parent objects.

Table 75 on page 169 lists the various audit change values that are listed in the **Action** column of the Audit Change Report with a brief description of the value and the affected object aspect.

<i>Table 75. Audit Change Report values</i>		
If the Status column has this value...	And the Item column has this value...	Then it indicates that...
Added	Association	An object was associated as a child object in the hierarchy.
Added	Object	A new object was created in the repository.
Added	Version	A new version of the object was created in the repository.
Changed	<property name>	The value of an object's system or extended property was modified.
Removed	Object	The object was logically deleted from the repository.
Removed	Association	An object was removed as a child object.
Removed Primary	Association	The association has been changed to Non-Primary. This could happen if the user selects another object relationship to be the Primary parent-child association or the current Primary association was deleted.
Added Primary	Association	The association type is set to Primary. This first association is always set to Primary

<i>Table 76. Audit Reports Configuration subfolder</i>	
Report Name	Description
Configuration Audit	Lists all configuration changes made to the OpenPages with Watson application during the chosen date range.

Table 77. Audit Reports Security subfolder

Report Name	Description
Administrator Permissions	Lists each administrator and their granted permissions for each Security Domain they administer.
Security Domain Role Assignments	Lists each Security Domain to which the selected roles are assigned.
Login Activity Summary	Lists all users who accessed the OpenPages with Watson system during the date range. Each user is listed with the last login time, when they last changed their password, and how many times they logged in.
Login Activity Log	Lists all user activity during the specified date range. Report users can filter on date range, operation (log in or log out), login status (Failed or Succeeded), and number of login attempts.
Roles by Security Domain	Lists each role that is assigned to the selected Security Domain.
Roles by User	Lists each user and group with their assigned role for the selected Security Domain.
User Role Assignments	Lists all the roles in the system with the assigned user or group for each Security Domain.

Issue Reports folder

The following table identifies the Issue reports available in the Issue Reports folder:

Table 78. Issue Reports

Report Name	Description
Issue List	Detailed listing of Issues and associated parent objects, which are filtered by reporting period and Business Entity. Note: This report shows a subset of the Issues present in the system. To appear in this report, Issues must be associated with objects that are accessible through direct relationships in the default namespace. For example, Issues that are associated with Controls that are indirectly associated with a Risk Assessment will not appear. Issues associated with Risks that are directly associated in a chain, from Business Entity to Process or Subprocess to Control Objective, appear.
Issues and Action Items	Lists Issues and associated Action Items for the chosen reporting period and Business Entity. Note: This report shows a subset of the Issues and Action Items present in the system. To appear in this report, Issues must be associated with objects that are accessible through direct relationships in the default namespace. For example, Issues associated with Controls that are indirectly associated with a Risk Assessment will not appear, while Issues associated with Risks that are directly associated in a chain, from Business Entity to Process or Sub-process to Control Objective, will appear.

Running reports (Task Focused UI)

In the Task Focused UI, you can run reports that have been configured to display in the Task Focused UI.

Before you begin

Configure the Task Focused UI to display reports. For more information, see [“Home page, dashboard, and tabs in the Task Focused UI”](#) on page 367 and [“Defining a dashboard for a profile”](#) on page 368.

About this task

For information about using the Task Focused UI, see the *IBM OpenPages with Watson User Guide*.

Running reports (Standard UI)

In the Standard UI, you can run all supplied reports and reports that you create.

They are typically found in the /openpages folder.

Procedure

1. From a browser window, log on to the OpenPages with Watson Standard UI.
2. Select **Reporting** on the menu bar and choose a report from the list. A separate browser window opens with the selected report.

If you selected the All Reports option, the Reports page is displayed. From the list on the Reports page, click the name of the report you want to launch.

Note: Depending on your configuration, application, and permissions, you may see different reports and folders.

3. If this is a "scoped" report, at the prompt, choose the object where you want the report to run from. For example, if you select a business entity, then the report will use the selected business entity as the starting point and limit the scope of the report to all objects contained below that entity.

If the report is not scoped, it will run as soon as you click the name of the report.

Adding reports to OpenPages with Watson

To run a report from either the Task Focused UI or the Standard UI, the report must first have a corresponding report page published to the OpenPages with Watson server.

A report page does the following:

- Adds a link on the Reporting menu and All Reports page to launch the Cognos report from the OpenPages with Watson Standard UI
- Specifies the parameters for launching the report
- Specifies the keys used for localizing the report name and description in the OpenPages with Watson user interface

All Cognos report pages are based on the CommandCenter Report page template, and all Cognos Workspace report pages are based on the CommandCenter Dashboard Redirect page template. Additionally, all Cognos Analytics dashboard and story pages are based on the Cognos Analytics Dashboard Redirect page template. These templates are located at the root of the Reporting folder on the OpenPages with Watson server.

You can use the following methods to add new reports to the OpenPages with Watson:

- Method 1: use the Task Focused UI to manually create the required report page and publishing the report. This method is typically used for editing report pages and troubleshooting publishing issues.

For more information, see [“Method 1: Using the Task Focused UI to add and edit reports”](#) on page 172.

- Method 2: use the Standard UI to automatically generate the required report page and application text keys. This is the recommended method.

For more information, see [“Method 2: Using the Standard UI to add reports”](#) on page 179.

Regardless of the method you use to add the report, be sure to save it in a folder, for example, OpenPages V6. Do not save the report in the OPENPAGES_REPORTS_V6 reporting package. OPENPAGES_REPORTS_V6 is the reporting framework that is used for authoring reports.

Method 1: Using the Task Focused UI to add and edit reports

You can use the **Manage Pages and Templates** task in the Task Focused UI to manually create the required report page and publish the report.

This method is typically used for editing report pages and troubleshooting publishing issues. It is an alternative to using the Standard UI to add reports. It can be used to edit reports that were added by using the Standard UI.

You can also use the **Manage Pages and Templates** task to create folders, copy, move, and delete report pages and page templates.

Understanding reports

Reports are generated by combining report pages and page templates that provide necessary information about the filtering and sorting of the report contents, as well as the displayed name and description of the report.

Reports (both Cognos and JSP) are represented in a folder by a page template which lists the parameters that the source file needs in order to create a report. A report page is an instance of a page template, and contains a set of values for the parameters specified in the page template.

In this manner, a single page template can be supplied with multiple sets of values for its parameters. This allows the IBM OpenPages with Watson application to create multiple reports based on the same layout and internal logic. Each report page represents a report as viewed in OpenPages with Watson.

Report pages and page templates reside on the OpenPages with Watson server.

Note:

- Cognos reports can be published through the Standard UI. This method automatically generates a corresponding report page and application text keys for localizing the selected report. For details, see [“Adding reports to OpenPages with Watson”](#) on page 171.
- Reports that are placed under the Reporting/SOX folder structure on the application server are published to the U.S. English locale. To publish to a different locale, choose the /SOX folder under the locale you want (for example, ja_JP/SOX for the Japanese locale).
- All Cognos report pages are based on the Cognos Report Redirect page template, which is located at the root of the Reporting folder on the IBM OpenPages server.

Locating report files

Report files, such as report pages, page templates, and JavaServer Pages (JSP) reports, are located in the IBM OpenPages with Watson repository on the OpenPages with Watson server.

The OpenPages repository handles the data storage and access capabilities for the OpenPages with Watson application. To create, modify, or delete OpenPages reports, you must have an OpenPages with Watson account with permission to modify reporting folders. If you are not sure whether you have access to this functionality, contact your OpenPages administrator for additional information.

Accessing report pages and page templates (Task Focused UI)

In the Task Focused UI, you can access report pages and page templates for JSP reports.

Before you begin

The administrator must be a member of the **OPAdministrators** group to access report pages and page templates in the Task Focused UI. If you are not a member of this group, you are not allowed to view the **Manage Pages and Templates** menu item.

About this task

Use the **Manage Pages and Templates** task to navigate through a hierarchy of folders and files. Each folder represents a report grouping in the IBM OpenPages user interface. Each page file represents an OpenPages with Watson report.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure.

Manually creating an instance of a report in the (Task Focused UI)

To manually create an instance of a report, you use the Task Focused UI and create a report page based on a copy of an existing page template.

About this task

The new report page will display clickable links in the OpenPages with Watson Standard UI for running the new report.

Note:

- Cognos reports can be published through the Standard UI. This method automatically generates a corresponding report page and application text keys for localizing the selected report. For details, see [“Adding reports to OpenPages with Watson” on page 171](#).
- Reports that are placed under the Reporting/SOX folder structure on the application server are published to the U.S. English locale. To publish to a different locale, choose the /SOX folder under the locale you want (for example, ja_JP/SOX for the Japanese locale).
- All Cognos report pages are based on the Cognos Report Redirect page template, which is located at the root of the Reporting folder on the IBM OpenPages server.

Identifying the page template (Task Focused UI)

You can determine which existing report page you want to copy from or use as the basis of a new report page.

About this task

If you already know the page template that you want to use, skip to the next task. Otherwise, complete this task to determine which existing report page you want to copy from or use as the basis of the new report page.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to find the report that you want to copy or use and modify as the basis of a new report.

3. Click the name of the report page to open it.
4. In the **General** section, note the value in the **Template** field. You will need to either reference this template or make a copy of the referenced template.

Creating a report page (Task Focused UI)

To create a new report, you create a new report page based on a copy of an existing page template.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to the folder where you want the report page to be created.

For example, a report page for a new Cognos report in the U.S. English locale would be placed in the Reporting/SOX/OpenPages V6 folder.

Optionally, create a category folder for grouping the reports under the appropriate /SOX folder. For example, to create a new report grouping titled "My Custom Reports" on the Reporting menu and Reports page in the OpenPages with Watson Standard UI for the U.S. English locale, you could create a folder with the path Reporting/SOX/My Custom Reports. Any report pages placed in the folder will appear under that grouping in the reporting sections of the OpenPages with Watson Standard UI.
3. Select the folder with a check mark.
4. Click **Add Page**.
5. Enter a **Name** for the report.

Note: You will not be able to change the name of a report after it is created.

6. In **Template**, choose the page template that you want to use to create the report.
For Cognos reports, use the CommandCenter Report Redirect page template.
7. Enter a **Description** for the report.
8. Click **Save**.

The window expands to show more fields. The fields that are displayed vary depending on the template you choose. Click in each field to add a value or click **Edit Mode** to tab through the fields.

9. If this is a JSP report, skip to Step 11. Otherwise, for a Cognos Studio report based on the CommandCenter Report Redirect page template, do the following.
 - a) Select a value for each of the following fields:

Table 79. Cognos Report Redirect Selection Fields	
Field Name	Description
Report Type	The IBM Cognos Studio application used to develop the report. Valid values are: • report (for IBM Cognos Analytics - Reporting, this is the default value) • query (for Cognos Query Studio) • analysis (for Cognos Analysis Studio) • pagelet (for Cognos Workspace, a type of dashboard that can contain multiple content pieces, including reports, on a single page)

Table 79. Cognos Report Redirect Selection Fields (continued)

Field Name	Description
Open with	The method for opening the report. Valid values are: • CognosViewer - opens the report in view-only mode, this is the default value. • ReportStudio - opens the report in IBM Cognos Analytics - Reporting so it can be modified. • QueryStudio - opens the report in Cognos Query Studio so it can be modified. • AnalysisStudio - opens the report in Cognos Analysis Studio so it can be modified. • CognosWorkspace - enables the report to be opened in Cognos Workspace.
Report Format	The display format for the report. Valid values are: • HTML (This is the default value. This value is required for Cognos Workspace reports.) • PDF • XLS • XLWA
Show prompt page	Determines whether or not a prompt page is always displayed for a report. If the value is set to: • Yes - a prompt page is always displayed even if the report has no required prompts. • No - a prompt page only displays if it is required by the report design. This value is set by default.
Report Folder	The report folders must be syntactically correct and separated by forward slashes. The Team content folder is assumed, and does not need to be included in the Report Folder field. For example, the report folder could be Vision 2019/Workspaces.
Report Name	The report name must be the name that you want to appear in Cognos Analytics.

b) Skip to Step 12.

10. For a report based on the CommandCenter Dashboard Redirect page template, do the following:

a) Click the **Mode** arrow and select the method for opening the dashboard.

Valid values are:

- view (opens the dashboard in view-only mode, this is the default value)
- edit (opens the dashboard in Cognos Workspace so it can be modified)

b) Skip to Step 12.

11. For a JSP report, enter the sorting and filtering information for the report.

12. Enter values for all required fields (required fields have a red asterisk *) including key field information as follows:

Table 80. Report Page Key Fields		
Key Field	Format	Description
Report Name Key	report.name.<user-defined> Example report.name.control.analysis	A key that references an application text string for localizing the title of the report.
Report Description Key	report.description.<user-defined> Example report.description.control.analysis	A key that references an application text string for localizing a description of the report.

Note: You can use the values in the **Report Name Key** and **Report Description Key** fields on the report page to manually create custom application text keys to localize the name and description of a report after it is created. For details, see [“The Custom folder” on page 576](#).

13. Click **Save**.

Results

When you log on to the Standard UI, the new dashboard or story should be visible in the selections on the Reporting menu.

Modifying a report page (Task Focused UI)

You can modify an existing report page.

Procedure

1. Click  > **System Configuration > Pages and Templates**.
2. Navigate through the folder structure to the folder that contains the report that you want to modify.
3. Click the report name.
4. Make your changes. Click in each field to change a value or click **Edit Mode** to tab through the fields.

Note: You cannot modify the name of a report. In order to change the name of a report, you must delete the misnamed report and create an identical report with the new name.

As an alternative, you can use the values in the Report Name Key and Report Description Key fields on the report page to manually create custom application text keys to localize the name and description of a report after it is created. For details, see [“The Custom folder” on page 576](#).

5. Click **Save**.

The modified information is saved and immediately applied to the dashboard or story.

Deleting a report (Task Focused UI)

About this task

You can delete an instance of a JSP report or report page for a Cognos report.

Procedure

1. Click  > **System Configuration > Pages and Templates**.
2. Navigate through the folder structure to the folder that contains the report that you want to delete.



Attention: Do not delete a page template. If a page template is deleted, all report pages based on that template are deleted as well.

3. Click **Delete**.
4. Click **OK** to delete the report page (or JSP report instance).

Manually creating an instance of a Cognos dashboard or story (Task Focused UI)

To manually create an instance of a Cognos dashboard or story, you must log on the Task Focused UI and create a dashboard or story page based on a copy of an existing page template.

The new dashboard or story page will display clickable links in the OpenPages with Watson Standard UI for running the new dashboard or story.

Note:

- Dashboards and stories that are placed under the Reporting/SOX folder structure on the application server are published to the U.S. English locale. To publish to a different locale, choose the /SOX folder under the locale you want (for example, ja_JP/SOX for the Japanese locale).
- All Cognos dashboard and story pages are based on the Cognos Analytics Dashboard Redirect page template, which is located at the root of the Reporting folder.

Identifying the dashboard or story page template (Task Focused UI)

You can determine which existing dashboard or story page you want to copy from or use as the basis of a new dashboard or story page.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to find the dashboard or story you want to copy or use and modify as the basis of a new dashboard or story.
3. Click the name of the dashboard or story page to open its detail page.
4. In the **General Information** section, note the value of the **Template** field. You will need to either reference this template or make a copy of the referenced template.

Creating a dashboard or story page (Task Focused UI)

To create a new dashboard or story, you must log on to the Task Focused UI and create a new dashboard or story page based on a copy of an existing page template.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to the folder where you want the dashboard or story to be created.

For example, a dashboard page for a new Cognos dashboard in the U.S. English locale would be placed in the Reporting/SOX/OpenPages V6 folder.

Optionally, create a category folder for grouping the dashboards or stories under the appropriate /SOX folder. For example, to create a new dashboard grouping titled "My Custom Cognos Dashboards" on the Reporting menu in the OpenPages with Watson application for the U.S. English locale, you could create a folder with the path Reporting/SOX/My Custom Cognos Dashboards. Any dashboard pages placed in the folder will appear under that grouping in the reporting sections of the OpenPages with Watson application.

3. Select the folder with a check mark.
4. Click **Add Page**.
5. Enter a **Name** for the dashboard or story.

Note: You will not be able to change the name of a dashboard or story after it is created.

6. In **Template**, choose the page template you will use to create the dashboard or story.
Cognos dashboards and stories use the Cognos Analytics Dashboard Redirect page template.
7. Click **Save**.
The window expands to show more fields. Click in each field to add a value or click **Edit Mode** to tab through the fields.
8. Select a value for each of the following fields:

Table 81. Cognos Analytics Dashboard Redirect Selection Fields	
Field Name	Description
Action	Select the method for opening the dashboard or story. Valid values are: • view (opens the dashboard or story in view-only mode, this is the default value) • edit (opens the dashboard or story in Cognos Workspace so it can be modified)
Mode	Select the page mode. Valid values are: • dashboard • story
Dashboard (or) Story Folder	The dashboard or story folders must be syntactically correct and separated by forward slashes. The Team content folder is assumed, and does not need to be included in the Dashboard (or) Story Folder field.
Dashboard (or) Story Name	The dashboard or story name must be the name that you want to appear in Cognos Analytics.

9. Click **Save**.

Modifying a dashboard or story template (Task Focused UI)

You can modify an existing dashboard or story template.

Important: If you want to modify the supplied dashboard and story template for your own purposes, you must copy it to a new location outside the SOX folder structure, and then modify the copied template. Otherwise, you will risk losing your changes when upgrading to a newer version of the IBM OpenPages with Watson application.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to the folder that contains the dashboard or story that you want to modify.
3. Click the dashboard or story name.
4. Make your changes. Click in each field to change a value or click **Edit Mode** to tab through the fields.

Note: You cannot modify the name of a dashboard or story. To change the name of a dashboard or story, you must delete the misnamed report and create an identical report with the new name.

As an alternative, you can use the values in the Report Name Key and Report Description Key fields on the report page to manually create custom application text keys to localize the name and description of a report after it is created. For details, see [“The Custom folder” on page 576](#).

5. Click **Save**. The modified information is saved and immediately applied to the report.

Deleting a dashboard or story (Task Focused UI)

You can delete an instance of a dashboard or story page for a Cognos dashboard or story.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to the folder that contains the dashboard or story that you want to delete.



Attention: Do not delete a page template. If a page template is deleted, all dashboard or story pages based on that template are deleted as well.

3. Click **Delete**.
4. Click **OK**.

Method 2: Using the Standard UI to add reports

You can add a report from the IBM OpenPages with Watson Standard UI.

When you add a report, the following process occurs:

- A corresponding report page is automatically generated on the OpenPages with Watson server that is based on the CommandCenter Report Redirect page template.
- The report is published, by default, to the U.S. English locale.
- If the report name and description are not specified for a locale, the values in the U.S. English locale are used by default.
- Report name and description application text keys are automatically created in the "Miscellaneous" folder on the **Application Text** page and populated with the specified values.

These key values are used for localizing the report name and description on the "My Reports" section of the home page and on the **Reporting** menu and page. To modify these key values, see [“Localizing application text” on page 564](#).

Before you begin

Before you can add a Cognos report from the Standard UI, you must have details about the report available.

- The name of the report. Do not enter special characters, including the underscore, in the report name.
- A description of the report
- The path and name of the folder to be deployed (the folder selection is filtered to list report folders only). By default, the path is `/_cw_channels/Reporting/SOX`.

Example

A new unpublished report was created called "My Control Summary" in the OPENPAGES_SHARED folder on the Cognos server. Publish the report to make it available for users in the US English and Japanese locales.

From the **Reports** page in the Standard UI, you click **Add** and select the report from the listing. For the US English locale (this locale is automatically selected by default), type in "My Control Summary" for the report name, and "All controls assigned to me" as the description for the report. You then select the Japanese locale and type in a localized name and description.

The application text keys for the "My Control Summary" report that are automatically generated under the "Miscellaneous" folder on the Application Text page may look similar to these: `report.name.openpages.shared.my.control.summary` and `report.description.openpages.shared.my.control.summary`.

You can use these keys to modify the report name or description that is displayed on the application user interface for a locale.



Attention: To view the new report on the Reports menu, users must log out and log back in to the application.

Report publishing limitations in the Standard UI

Publishing report pages from the Standard UI has some limitations.

- You can publish only one report at a time.
- If you want to edit existing reports, you must use the Task Focused UI to edit the report page. For more information, see [“Modifying a report page \(Task Focused UI\)” on page 176](#).
- If the initial publishing process failed to publish a report to any locale other than English, you must use the Task Focused UI to add the report. For more information, see [“Manually creating an instance of a report in the \(Task Focused UI\)” on page 173](#).

Accessing the publish report page (Standard UI)

To access the **Add** icon on the Reports page in the Standard UI, you must have the **Add Pages** application permission set on your account.

For details, see [“Types of application permissions” on page 91](#).

Procedure

1. From the menu bar, select **Reporting** and click **All Reports**.
2. Click **Add** to go to the **Publish Report** page.

Publishing a report (Standard UI)

The Report selection list in the Standard UI contains all available reports that are not already published.

Procedure

1. Access the **Publish Report** page (see [“Accessing the publish report page \(Standard UI\)” on page 180](#)).
2. Select a report from the Report list.
3. Select the check box for each locale in which you want the report to display. For example, German. The U.S. English locale is selected by default.
4. In the **Name** field for each selected locale, type the display name of the report.

This name will be displayed to users in the report selection list and on the Reports page, and, if configured on the Home page, in a tab or in a pane on the My Work tab.

5. In the **Description** field for each locale, type a description of the report. This description will be displayed to users on the Reports page.

Note: Any locale for which you do not specify a localized name and description will, by default, contain the U.S. English name and description.

6. When finished, click **Save**.

After the report is published, a link to launch the report is displayed on the Reports page along with a description of the report, and the report name is added to the list of selections on the Reporting menu.

Modifying the displayed report name or description

You can localize and modify the name and description that is displayed to users on the IBM OpenPages with Watson for a report in a given locale.

You do this by locating the application text keys that correspond to the name and description of the report and then modifying the value in the key for that locale.

For more information and instructions, see [“Modifying application text \(Task Focused UI\)” on page 566](#) or [“Modifying application text \(Standard UI\)” on page 567](#).

Creating an interactive JSP report (Task Focused UI)

The IBM OpenPages with Watson application allows administrative-level users with the option to create interactive reports to prompt a user at run-time for parameter values. You can either modify an existing JSP report to be interactive, or specify an interactive parameter during report creation.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to find the page template for the report that you want to modify.
3. Click the name of the page template you want to modify.
4. Scroll down to the **Parameters** section.
5. Click the name of the parameter that you want to make interactive.
The parameter information is displayed.
6. Set **Interactive Value** to true and click **Done**.
7. Repeat the steps for each parameter that you want to make interactive.
8. Click **Save**.

Results

The next time the report is run, the user will be prompted to enter a value for each field marked as an interactive value.

Important: Reports with an interactive parameter named "label" are a special case and will not display a dialog to enter a value for "label". The "label" field is included to support reporting periods and should not be modified.

Note: Although any parameter type can be defined as an interactive parameter that requires a user to provide information at run time, IBM OpenPages supports only the following four modes of entering values into the value fields when the report is run:

- Date fields
- Text entry fields
- Enumerated drop-downs
- File browsers

Unsupported types might be marked as interactive. However, the value for these fields must be entered manually, using a text string at run-time. A valid value must be entered into the value field for the report to return the correct set of information.

What to do next

For information about running an interactive report, see [“Running an interactive JSP report \(Standard UI\)” on page 182.](#)

Running an interactive JSP report (Standard UI)

The IBM OpenPages with Watson application allows administrative-level users with the option to create interactive reports to prompt a user at run-time for parameter values.

Note: Although any parameter type can be defined as an interactive parameter that requires a user to provide information at run time, IBM OpenPages supports only the following four modes of entering values into the value fields when the report is run:

- Date fields
- Text entry fields
- Enumerated drop-downs
- File browsers

Unsupported types might be marked as interactive. However, the value for these fields must be entered manually, using a text string at run-time. A valid value must be entered into the value field for the report to return the correct set of information.

Procedure

1. From a browser window, log on to Standard UI.
2. Select **Reporting** on the menu bar, and select the name of the report you want to run. If the report contains interactive parameters, a prompt page is displayed.
3. Type information into the required fields.
4. Click **Next** to generate the report based on the supplied information. The report is displayed in a new window.

Restricting access to reports in the Task Focused UI

To restrict access and set security on reports, you need to set permissions in the IBM OpenPages with Watson Task Focused UI and in IBM Cognos Analytics.

Note: If you restrict access to reports only through IBM Cognos Analytics, but not in the Task Focused UI, the reports may be displayed in a selection list to users in the Standard UI. If a group or user who does not have permission selects the restricted report, the report will not run and an error message will be displayed to the user.

Setting permissions on JSP and reports in the Task Focused UI

You can restrict users and or groups from accessing and running JSP reports from the OpenPages with Watson Standard UI by setting Read, Write, Delete, and Manage permissions on selected report folders.

About this task

For example, if you want only administrators in a System Administrators group to have access to administrative reports, you could set Read, Write, Delete, and Manage access on the Administrative Reports subfolder (which is under the SOX >> Cognos folder). After you grant access to administrative reports for the System Administrators group, you can then break inheritance on the folder to restrict other users and groups from accessing these reports.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure. Expand the folders, if necessary.

Note:

- Each folder represents a report grouping in the OpenPages with Watson Standard UI.
 - Reports that are under the Reporting/SOX folder structure are published to the U.S. English locale. To select a different locale, choose the /SOX folder under the locale you want (for example, ja_JP/SOX for the Japanese locale).
3. Click on the name of the folder that contains the reports to which you want to limit access.
The folder properties are displayed.
 4. Scroll down to the **Access Control** section.
 5. Click **Add Access Control**.
 - a) Select a group or user to whom you want to grant permission.
 - b) Select the permissions you want to allow or deny the group or user (Read, Write, Delete, Manage).
 - c) Click **Add**. The selected group or user appears in the list.
 - d) To select another group or user, repeat Steps a-c.
 - e) To remove a group or user, select the group or user then select **Remove**.
 6. Break inheritance on the folder so that other groups or users cannot access these reports from the OpenPages with Watson Standard UI:
 - a) In the properties for the folder, set **Inherit ACL** to false.
 7. Click **Save**.

Securing access to the report portal

You can restrict which user groups are allowed to modify CommandCenter reports.

Note: This task is optional.

Use the following tasks to allow a group, in this example the 'OPAdministrators' group, to update, add, and delete reports, and to restrict other users from changing settings within the IBM Cognos Analytics:

- [“Assigning CommandCenter administrative rights to a group” on page 183](#)
- [“Specifying user access to administrative functions in the IBM Cognos Analytics” on page 184](#)
- [“Restricting access to reports in Team content folder” on page 184](#)
- [“Restricting users to only running reports” on page 185](#)

Note: IBM OpenPages with Watson standard reports could be overwritten during an upgrade. If you want to modify the standard reports, it is best that you copy the reports to your own folder structure where you can then modify and control access to these reports.

Assigning CommandCenter administrative rights to a group

Before you can specify access rights and restrictions to reports and reporting functions, you must assign CommandCenter administrative rights to a new or existing group.

Procedure

1. From a browser window, log on to the Task Focused UI as a user with administrative privileges.
2. Create a group in to which you want to give CommandCenter administrative rights, or use an existing group, such as OpenPagesAdministrators.

Note: For information on creating groups, see [“Creating an organizational group \(Task Focused UI\)” on page 88](#).

Specifying user access to administrative functions in the IBM Cognos Analytics

You can specify which users have access to administrative functions within the IBM Cognos Analytics.

Procedure

1. From a browser, log on to the IBM Cognos Analytics as a user with administrative privileges, for example, OpenPagesAdministrator.

By default, the URL is:

`http://<hostname>/ibmcognos/bi` (if you are using port 80 for Cognos)

Where <hostname> is the name of the Cognos server.

2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Security** tab, click the **Cognos** link in the **Directory** list.
4. On the **Directory > Cognos** page:
 - a) Locate the System Administrators group in the list.
 - b) Click the **More** link in the same row as the System Administrators group.
5. Under **Available Actions** on the **Perform an Action** page, click the **Set members** link.
6. On the **Members** tab of the **Set Properties** page, click the **Add** link.
7. On the **Select entries (Navigate)** page, do the following:
 - a) Click the **OpenPagesSecurityRealm** link to find the IBM OpenPages with Watson group or role to access CommandCenter administrative functions.
 - b) Select a group. For example, OPAdministrators.
 - c) Click the green arrow to add the role.
8. On the **Members** tab of the **Set Properties** page, restrict access to the administrative functions.
 - a) Select the Everyone group.
 - b) Click the **Remove** link.

Restricting access to reports in Team content folder

You can restrict users to only being able to access reports that are in the **Team content** folder.

Procedure

1. On the Cognos Analytics page, click the **Team content** folder.
2. On the **Team content** page, click the **More** link in the same row as the IBM OpenPages with Watson folder for which you want to restrict access (for example, OPENPAGES_REPORTS_V6 or FCM_REPORTS).
3. Under **Available actions**, click the **Set properties** link.
4. On the **Set properties** page, select the **Permissions** tab and do the following:
 - a) If not already selected, select the box to Override the access permissions acquired from the parent entry.
 - b) Click the **Add** link (located near the end of the page).
5. In the **Select entries (Navigate)** window, click the **Cognos** link, and do the following:
 - a) Select the group to be added (for example, System Administrators).
 - b) Click the green arrow to add the role.
6. On the **Permissions** tab of the **Set Properties** page, do the following:
 - a) Select the box next to the newly added group (for example, System Administrators).

- b) Grant the group Read, Write, Set Policy, and Traverse permissions.
- c) Remove the Write and Set Policy permissions from the other groups.

Now, if a user logs on to CommandCenter with a user name that is not in, for example, the OPAdministrator group, and the user tries to delete, change, or save a report, for example, in the OPENPAGES_REPORTS_V6 or FCM_REPORTS package, an error message is displayed to the user.

Restricting users to only running reports

You can restrict users to only run reports, with no access to IBM Cognos Analytics - Reporting to modify reports.

Procedure

1. From a browser, log on to the IBM Cognos Analytics as a user with administrative privileges, for example, OpenPagesAdministrator.
By default, the URL is:
`http://<hostname>/ibmcognos/bi` (if you are using port 80 for Cognos)
Where <hostname> is the name of the Cognos server.
2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
3. Select the **Security** tab, and click the **Cognos** link in the **Directory** list.
4. On the **Directory > Cognos** page, click the **More** link in the same row as the "Authors" role.
5. On the **Perform an action** page, under **Available Actions**, click the **Set members** link.
6. On the **Members** tab of the **Set properties** page, click the **Add** link.
7. On the **Select entries (Navigate)** page, do the following:
 - a) Click the **OpenPagesSecurityRealm** link.
 - b) Select the group you want (for example, OPAdministrators).
 - c) Click the green arrow to add the group and then click **OK**.
8. On the **Members** tab of the **Set Properties** page:
 - a) Select the **Everyone** group
 - b) Click **Remove**.
9. Repeat Steps 2 - 6 for the "Query User" role.
10. When finished, return to the **IBM Cognos Administration** page and select the **Security** tab.
11. On the **Security** tab, click the **Capabilities** link, and do the following:
 - a) Click the **Report Studio** link.
 - b) Click the **Actions** arrow next to **HTML Items in Report** and select **Set properties**.
12. On the **Set properties - HTML Items in Report** page, do the following:
 - a) Select the **Permissions** tab.
 - b) If not already selected, select the box to "Override the access permissions acquired from the parent entry".
13. In the list on the **Permissions** tab, select the "Everyone" group and grant the group Execute and Traverse permissions.
Note: If the "Everyone" group is not listed, then add it to the list as follows:
 - a. Click the **Add** link.
 - b. On the **Select entries (Navigate)** window, click the **Cognos** link.
 - c. Select the "Everyone" group.
 - d. Click the green arrow to add the role.

- e. Select the "Everyone" group and grant the group Execute and Traverse permissions.
14. Return to the **Security** tab and do the following:
- a) Click the **Capabilities** link again.
 - b) Click the **Report Studio** link.
 - c) Click the **Actions** arrow next to **Create/Delete** and select **Set properties**.
15. On the **Set properties - Create/Delete** page, do the following:
- a) Select the **Permissions** tab.
 - b) If not already selected, select the box to "Override the access permissions acquired from the parent entry".
 - c) Remove the "Everyone" group, if it is listed there.
 - d) Add the "System Administrators" group with Read, Write, Set Policy, and Traverse permissions.

Results

After completing this procedure, the user cannot modify reports but can still run out-of-the-box reports.

Chapter 8. System file management

The ability to manage system folders and files is essential for information management in IBM OpenPages with Watson.

Using the **System Files** area of OpenPages you can complete the following tasks:

- View folders and files
- Manage folders and files
- Search for files

Object types

The **System Files** area of OpenPages contains seven types of system files (content file types). Six types are unique system file types, but the seventh type, Files (SOXDocument), can be either system files or non-system files.

The content file types are defined as the following seven object types in OpenPages:

- Files (SOXDocument)
- SysXMLDocument
- ExporterXML
- MigrationJAR
- ModelConnectionConfig (legacy)
- Report
- VizConfig (legacy)

You manage these object types like other object types in the system. Do not disable the Folder View for these object types (Standard UI only).

Table 82. Object types for files	
Object type	Description and examples
Files (SOXDocument)	System and non-system files • DefaultTemplate.xls (example of a system file) • attachments that users add to objects (examples of non-system files)

Table 82. Object types for files (continued)

Object type	Description and examples
SysXMLDocument	End user application configuration JSON and trigger configuration files • The SysXMLDocument folder contains the <code>_trigger_config.xml</code> file. • The TriggerConfigFiles folder contains trigger configuration files, such as: <code>openpages-solutions.xml</code>, <code>OPLC-QuestionnaireAssessment.xml</code>, <code>OPLC-Incident.xml</code>, and so on. The trigger configuration files must also be listed in the Applications > GRCM > Trigger Configuration Files setting. For more information, see the <i>IBM OpenPages with Watson Trigger Developer Guide</i>. • The End User Applications Config folder contains end user application configuration files such as: – Approval app: <code>deck_config.json</code> – IBM OpenPages Loss Event Entry: <code>lossevent_config.json</code> – Natural Language Classifiers: the <code>classifiers</code> folder contains json files. Each file contains connection information for an instance of a Natural Language Classifier. For more information, see “Defining a Classifier Configuration (Task Focused UI)” on page 1028. • The Taxonomy folder contains taxonomy files, which are used by IBM OpenPages Regulatory Compliance Management.
ExporterXML	Notification reports Expand the <code>_exporter</code> folder to see the files.
MigrationJAR	JAR files that are imported by using Administration > Import Configuration and exported by using Administration > Export Configuration Expand the Migration Documents folder to see the files. Example: <code>openpages-env-mig_<timestamp>.jar</code>
ModelConnectionConfig	Visual diagram files (legacy)
Reports	JSP files, for example, solution helpers, Command Center redirects, FastMap reports, and more Expand the Reports folder to see the report files. Example: <code>Reports/SOX/ORM Custom Reports/ORM_IMRBulletin.jsp</code>
VizConfig	Visualization configuration files (legacy) Expand the <code>_vizConfig</code> folder to see the files. Examples: • <code>EntityDetail.json</code> • <code>EntityHierarchy.json</code> • <code>ProcessFlow.json</code>

Access permissions for folders and files

Not all folders and files are accessible to all users. Each folder and file can have its own set of access permissions that determine which users are allowed to view or edit it. Sensitive or private information remains visible only to selected users, most often to prevent accidental editing or deletion.

Each user can view only the folders and files to which they have access permissions. Each user's view of the file system can appear differently, although all users are typically working from the same set of data. For example, one user can have access to all folders and files and be able to see all files in the system. Another user can have access to only a limited set of folders and files, which makes the folders and files to which they do not have access uneditable.

Note: The creator of a file is automatically granted all access permissions to that file, regardless of the limitations set by a group or the folder where the file is located.

Access to the System Files menu item

The OpenPages Platform 3 profile includes access to all of the system file types. An administrator assigned this profile has access to all the system files and folders.

Add the ready-to-use OpenPages Platform 3 profile to the list of available profiles for your administrators who manage system files. Using this profile, you have access to the **System Files** menu items in both user interfaces. You also have access in the Standard UI to the Detail, Folder, and Filter list views for the object types for system files.

If you do not use the OpenPages Platform 3 profile, you can add the system file object types to any other profiles that administrators use. Users must be members of the OPAdministrators user group for the **System Files** menu item to display.

Version control in the file repository

OpenPages uses version control and file locking in the file repository. When you work in a collaborative team environment, files are checked in and out to ensure that changes made by one team member will not be overwritten by another team member.

When you add a file, a copy of the file is uploaded to the OpenPages file repository. After a file has been added:

- Click the file name to view file details and access multiple versions of the file if they exist.
- Click  to download it.

Click **Check Out** to check out a file.

A checked-out file has the following characteristics:

- A check mark is displayed next to the file name. If it is green, you checked it out. If it is blue, it is checked out by another user (Task Focused UI only).
- The file is locked and cannot be overwritten in the file repository.
- The last checked in version and all earlier versions of the file can be viewed and downloaded by other users.

When you check in a file, you can add a comment. A new version is then uploaded with your latest changes, the file is unlocked, and it is available to other users to view and check out.

Accessing files and folders in the Task Focused UI

System files and folders are accessed with the  > **System Configuration** > **System Files** task.

Non-system files are accessed with the **Attachments** > **Files** task. Users can also add non-system files directly to objects from Task Views.

Disregard and do not use the  > **Manage System Files** menu item.

Table 83. Where to access files in the Task Focused UI

To access this type of file ...	Go to ...
Files (SOXDocument)	 > System Configuration > System Files (system files) or Attachments > Files (non-system files)
SysXMLDocument	 > System Configuration > System Files and then expand the End User Applications Config folder or Trigger Config Files folder
ExporterXML	 > System Configuration > System Files and then expand the _exporter folder
MigrationJAR	 > System Configuration > System Files and then expand the Migration Documents folder
ModelConnectionConfig	No access in the Task Focused UI.
Reports	 > System Configuration > System Files and then Expand the Reports folder
VizConfig	 > System Configuration > System Files and then Expand the _vizConfig folder

Accessing files and folders in the Standard UI

System files and folders are accessed from the **Administration** > **Manage System Files** menu.

Non-system files are accessed with the **My OpenPages** > **Files** task. Users can also add files directly to objects.

The following video explains how to configure the ability to manage system files using the Standard UI:

<https://youtu.be/pJrrWNwpXuY>

Table 84. Where to access files in the Standard UI

To access this type of file ...	Go to ...
Files (SOXDocument)	Administration > Manage System Files > Files (system files) and My OpenPages > Files (non-system files)
SysXMLDocument	Administration > Manage System Files > SysXMLDocument and then expand the End User Applications Config folder
ExporterXML	Administration > Manage System Files > ExportXML and then expand the _exporter folder
MigrationJAR	Administration > Manage System Files > MigrationJAR and then expand the Migration Documents folder
ModelConnectionConfig	Administration > Manage System Files > ModelConnectionConfig
Reports	Administration > Manage System Files > Reports
VizConfig	Administration > Manage System Files > VizConfig

Comparison of OPX administrative interface to Manage System Files

Reporting folders, report pages, and page templates are maintained by using  > **System Configuration** > **Pages and Templates** in the Task Focused UI. They are not available in **System Files**. In previous releases, reporting folders, report pages, and page templates were maintained in the OPX administrative interface. OPX administrative interface has been removed from OpenPages.

In the Standard UI, SOXDocument system files are accessed in **Administration** > **Manage System Files** > **Files**. SOXDocument non-system files are accessed in **My OpenPages** > **Files**. In the OPX administrative interface, the SOXDocument system and non-system files were in the same location.

If you are familiar with how files and folders were organized in the OPX administrative interface, the following table explains where you can find the most commonly used system files in **Administration** > **Manage System Files** in the Standard UI:

Table 85. Comparison of OPX to Manage System Files	
These files in OPX...	Are located in ...
Trigger configuration files	Administration > Manage System Files > SysXMLDocument
End user application configuration files	Administration > Manage System Files > SysXMLDocument
FLV export spreadsheet template files	Administration > Manage System Files > Files

Known issues in the Standard UI

The following behaviors are known issues in **Administration** > **Manage System Files** in the Standard UI:

- If you set up filters for SysXMLdocument files for the Analytics bar, the filter correctly displays the results but incorrectly calculates as zero the number of results available.
- In Folder View, only system files under the current reporting period are displayed. If you click a system file folder and select a finalized reporting period, no files in the folder are displayed and an error is shown.
- In Detail View for a system file, you can choose only **Current** in **Reporting Period**. You cannot choose a finalized reporting period.
- If you apply a filter in **Administration** > **Manage System Files**, the filter is not automatically applied in **My OpenPages** > **Files**, and vice versa.
- You must disable System Admin Mode to add new system files.

System file management tasks

To enable you to manage your content effectively, changes often have to be made to your folder and file structure, including changing file locations, changing file and folder names, and removing unwanted content from IBM OpenPages with Watson.



CAUTION: System files must have specific names and be in specific folders so use caution when moving, deleting, or renaming these types of files or their folders.

Managing system files and folders (Task Focused UI)

Use the  > **System Configuration** > **System Files** task to manage system files and folders.

Whether the  > **System Configuration** > **System Files** menu item is displayed depends on your access permissions. When you click it, a list of system files and folders is displayed.

Working with files

From the list of system files and folders, you can work with files:

- Click  to search for files by object type.
- Expand and collapse folders to navigate to the file you want to work with.
- Select the check box next to a single file. The bulk update options are:
 - **Rename**
You can rename a folder or file only if you have the correct permissions to do so.
 - **Copy**
 - **Move**
 - **Delete**
- Select the check box next to multiple files to update numerous files. The bulk update options are:
 - **Copy**
 - **Move**
 - **Delete**
- Add, download, and modify system files. For more information, see [“Adding and modifying system files \(Task Focused UI\)” on page 195](#)

Working with folders

From the list, you can work with folders:

- Click a folder name. The folder details and access controls are displayed.
- Select the check box next to a single folder. The bulk update options are:
 - **Add New** (to add a new file to the folder)
 - **Add Folder** (to add a new folder)
You can create a new folder within any folder for which you have access permissions.
 - **Copy**
- Select the check box next to multiple folders to update numerous folders. The bulk update options are:
 - **Copy**

Moving files and folders

If you attempt to move a file into a folder that already contains a file with the same name, the file will not be moved. If you paste the file into a folder that does not already contain a file with the same name, then the original file name will be used.



CAUTION: Because some files are referenced by other system processes, and because other users may be working with common files, ensure that you are not going to inadvertently disrupt the work or files of others before moving a file.

Deleting files and folders

When you delete a folder, the folder and all of its contents are removed from IBM OpenPages with Watson. When you delete a file, it is removed from OpenPages. You can only delete a folder or file if you have the appropriate access permissions.



CAUTION: Because some folders and files are referenced by other system processes, and because other users may be working with shared files, please ensure that you are not going to inadvertently disrupt the work of others before deleting content.

Assigning access control to folders

You can control which users and groups can access files. Access controls (ACL) are defined at the folder level and apply to all files within the folder. They are defined by users and groups.

Click a folder. Then click **Add Access Control**. Select a user or group. For each permission (Read, Write, Delete, Manage), select a setting value (Granted, Inherited, or Denied).

Opening files and folders in a Quick View

Click  to open a file or folder in a Quick View. The file or folder opens in the side panel.

All of the functionality that is available in the folder view is also available in a Quick View with the following exception:

- Files cannot be checked in, checked out, or uploaded.

Click  to open the file or folder in its own tab. Full functionality is then available.

Creating folders (Standard UI)

In IBM OpenPages with Watson, you can create a new folder within any folder for which you have access permissions.

Procedure

1. Go to **Administration > Manage System Files**.
2. Select the system file type.
3. Select the check box next to the folder that you want to add the new folder to.
4. Click **Add Folder**.
5. Type a name and description for the folder.
6. Click **OK**.

Uploading files (Standard UI)

You can add files to folders in IBM OpenPages with Watson.

Procedure

1. Go to **Administration > Manage System Files**.
2. Select the system file type.
3. Select the check box next to the folder that you want to upload the file to.
4. Click **Add New**.
5. Click **Choose File** and select the file that you want to upload.
6. Type a description for the file.
7. Click **Create**.

Moving files or folders (Standard UI)

IBM OpenPages with Watson enables you to move files or folders from one location in the folder hierarchy to another.

About this task

If you attempt to move a file into a folder that already contains a file with the same name, the file will not be moved. If you paste the file into a folder that does not already contain a file with the same name, then the original file name will be used.



CAUTION: Because some files are referenced by other system processes, and because other users may be working with common files, ensure that you are not going to inadvertently disrupt the work or files of others before moving a file.

Procedure

1. Go to **Administration > Manage System Files**.
2. Select the system file type.
3. Select the check box next to the file or folder that you want to move.
4. Click **Move To**.
5. Navigate to the folder that you want to move the file to.
6. Click **OK**.

Copying files and folders (Standard UI)

You can copy files and folders to a different folder in IBM OpenPages with Watson.

Procedure

1. Go to **Administration > Manage System Files**.
2. Select the system file type.
3. Select the check box next to the file or folder that you want to copy.
4. Click **Copy To**.
5. Navigate to the folder that you want to move the file to.
6. Click **OK**.

Renaming files or folders (Standard UI)

IBM OpenPages with Watson enables you to rename folders and files in the system. You can only rename a folder or file if you have the correct permissions to do so.

Procedure

1. Go to **Administration > Manage System Files**.
2. Select the system file type.
3. Select the check box next to the file or folder that you want to rename.
4. Click **Rename**.
5. Type a new name and click **OK**.

Deleting files or folders (Standard UI)

When you delete a folder, the folder and all of its contents are removed from IBM OpenPages with Watson. When you delete a file, it is removed from OpenPages. You can only delete a folder or file if you have the appropriate access permissions.

About this task



CAUTION: Because some folders and files are referenced by other system processes, and because other users may be working with shared files, please ensure that you are not going to inadvertently disrupt the work of others before deleting content.

Procedure

1. Go to **Administration > Manage System Files**.
2. Select the system file type.
3. Select the check box next to the file or folder that you want to rename.
4. Click **Delete**.

System file modification

You can download a copy of a file to view if you have view permissions for the file or you can edit a file by checking it out of IBM OpenPages with Watson.

When you check in an updated file, the original file is updated in OpenPages with the newer edited version. If file versioning is enabled, then older versions of files are maintained as you make edits. The most recently checked in version of a file is considered as the current version.

Adding and modifying system files (Task Focused UI)

Use the  > **System Configuration > System Files** task to add and modify system files.

About this task

By default in 8.2.0.2 and later, only super administrators and members of the OPAdministrators group can create or modify system JSP files in the /Report folder.

For more information about system files and folders, see [“Managing system files and folders \(Task Focused UI\)” on page 191](#).

Procedure

1. Click  > **System Configuration > System Files**.
2. To add files to a folder:
 - a) Navigate to the folder where the file will be saved.
 - b) Select the check box next to a folder and click **Add New**.
 - c) Select an object type:
 - File (SOXDocument)
 - SysXMLDocument
 - ExporterXML
 - ModelConnectionConfig
 - MigrationJAR
 - Report
 - VizConfig

- d) Enter a **Description**.

Fields and button labels vary depending on the object type you chose. They may also vary depending on how your system is configured.

- e) Click **Add File** and select the file. Only file types that match the object type are available to be selected.
- f) If you chose File for object type, click **Select Folder** and associate the file to a parent business object. You might also be able to add keywords and select a document type.
- g) Click **Save**.

The file is added and automatically checked in.

After a file has been added, there are two methods to upload a new version of it. Using either method, you receive an error message when you upload the file if it is checked out by another user.

- 3. To update a file using manual check out:

Use this method to prevent other users from editing the file while you are working on your changes.

- a) Click a file.
- b) Click **Check Out**. The icon is hidden if the file is already checked out.
- c) Download the file.
- d) Make and save your changes to the file.
- e) Click **Update** and select the file. Alternatively, you can drag the file to the page.
- f) Complete the fields in the **Files to update** pop-up window.
- g) Click **Upload**. Your copy is uploaded and checked in.

You can click **Cancel Check Out** to cancel a check out. If you cancel a check out, OpenPages reverts to the last checked in version of a file in the file repository.

- 4. To update a file without using manual check out:

Use this method if you are making quick changes to the file.

- a) Click a file.
- b) Download the file.
- c) Make and save your changes to the file.
- d) Click **Update** and select the file. Alternatively, you can drag the file to the page.
- e) Complete the fields in the **Files to update** pop-up window.
- f) Click **Upload**. The file is automatically checked out and back in.

Downloading files (Standard UI)

You can view a file stored in IBM OpenPages with Watson by downloading it to your computer.

Procedure

1. Go to **Administration > Manage System Files**.
2. Select the system file type.
3. Navigate to the file that you want to download.
4. Click the file.
5. In the **Name** field, click **View file**.

The file is downloaded to your computer.

Checking out files (Standard UI)

You can edit a file by checking it out of IBM OpenPages with Watson.

About this task

While a file is checked out, it is locked in OpenPages, thereby preventing any other user from making changes while you have the file checked out.

Procedure

1. Go to **Administration > Manage System Files**.
2. Select the system file type.
3. Navigate to the file that you want to check out.
4. Click the file.
5. From the **Actions** drop-down menu, select **Check out this <type of system file>**.

The file is now locked.

6. In the **Name** field, click **View file**.

The file is downloaded to your computer and available for edit.

Uploading modified files (Standard UI)

After you have made changes to a checked out file, you must upload the revised file to IBM OpenPages with Watson.

Procedure

1. Go to **Administration > Manage System Files**.
2. Select the system file type.
3. Navigate to the file that you want to upload the newest version of.
4. Click the file.
5. From the **Actions** drop-down menu, select **Edit/Upload this <type of system file>**.
6. Click **Choose File** and select the new version of the file.
7. Click **Save**.

Checking in files (Standard UI)

After you have edited and uploaded a file you can check it back in to IBM OpenPages with Watson.

About this task

When you check a file back in, it becomes unlocked, and may then be edited by other users.

If you are checking in a trigger configuration file, [refresh the trigger configuration](#) to apply your changes.

Procedure

1. Go to **Administration > Manage System Files**.
2. Select the system file type.
3. Navigate to the file that you want to check back in.
4. Click the file.
5. From the **Actions** drop-down menu, select **Check in this <type of system file>**.

The file is now unlocked.

Refreshing trigger configurations

In IBM OpenPages with Watson, you can use the Trigger Configuration Refresh Utility to apply new or updated trigger XML configuration files as well as changes to the triggers registry settings.

About this task

By default, only users in the OPAdministrators group and the OpenPagesAdministrator users have access to this utility. Running this utility refreshes the trigger cache. Updates to JAR files are not refreshed by this utility. The application server must be restarted for new JAR files to be loaded.

In the Standard UI, you can access this utility with the **Reporting > OpenPages V6 > Configuration Utilities** task.

Procedure

1. Click  > **System Configuration > Pages and Templates**.
2. Go to **Reporting > <Locale> > SOX > OpenPages V6 > Configuration Utilities**.
3. Select **Trigger Configuration Refresh Utility**.

Chapter 9. Fields and field groups

A field group is a container for fields. Each field must belong to a field group.

You can add new fields to object types and custom forms, and manage existing fields.

If a field is defined as a simple string or long string data type, you can also encrypt the field values in the IBM OpenPages with Watson repository.

To manage new fields, either add new fields to an existing field group or create a new field group and add the fields to it.

Fields and field groups can be defined and managed using tasks in either the Task Focused UI or the Standard UI. Changes made in one interface are immediately reflected in the other. Functionality between the two user interfaces is mostly the same except for the following differences:

- In the Task Focused UI, the Display Type attribute is defined directly on fields. In the Standard UI, the Display Type attribute is defined on profiles.
- In the Task Focused UI, there are two additional data types:
 - Business entity selector
 - User/group

These data types do not exist in the Standard UI. Instead, they are defined as display types for simple string fields.

In the Standard UI a field group is identified by the **Field Group** icon . An object field is identified by the **Object Field** icon .

Definition of fields

An object field represents information that is specific to an object type.

Fields can be object fields, computed fields, and report fragment fields.

By default, each object type has a predefined field group that contains fields that are specific for that object type. For example, the "Effectiveness Rating" and "Operating Effectiveness" fields belong to the Control object field group called OPSS-Control.

Fields are added to a new or existing field group. They are then associated with a profile.

If you create a new object type for a custom form or survey, you must add field groups to that object type. Field groups are new or existing field groups. For more information, see [“Adding an object type for a custom form” on page 265](#).

丈, 巳, ㄣ, 乙, 卩, 工,
鷄, 騰, 鷄, 鷄, 鷄

Important: Do not use the four-byte characters that are defined
in the CJK Unified Ideographs EXTENSION-B Unicode Block Name in field values. These characters will
not be saved.

Definition of a field group that is in use

When a field group is associated with an object type, an instance of the object type is created. The field group is in use.

When a field group is in use, you cannot delete the field group or any fields from that field group. You also cannot exclude the field group from an object type.

For example, you create a new field group that is called Extra Fields with three object fields, called Field 1, Field 2 and Field 3. You then add the new field group to the Risk object type. Even if you never display any of the new fields on any Risk object view page, the Extra Fields field group is in use and cannot be deleted.

Note: If a management operation is being modified by two administrators at the same time, an error message is displayed, notifying you to try again later.

Requirements for new fields

Before you create a new field, determine the characteristics of the field and the object types that will use the new field.

The following list identifies information that is needed before you create a new field:

- Object - Will the new field be added to a custom form or object? For objects, identify the object types where the new field will be added.
- Name - How will the new field be identified? The name is important because it is also the label that appears next to the field. Special characters cannot be used. For additional information, see [“Field naming guidelines”](#) on page 201.
- Label - What text is displayed when this field appears on an object View page? The initial label is the same as the name of the field. For example, if this field is added to the Detail view page of an object, it is also displayed on the Add and Edit pages. If required, modify the label text. For more information, see Chapter 17, [“Localizing text,”](#) on page 559).
- Data type - What is the type of data, such as Boolean or Date that is captured by the field? For more information, see [“Data types”](#) on page 203.
- Entry type - Is the user required to enter data in the field or is data entry optional? For more information, see [“Making fields required or optional”](#) on page 209.
- Default value - Is a default value defined or is it blank?
- Encrypted - If the field is defined as a simple string or long string data type, decide if the field values should be further secured by using encryption. For more information, see [“Encrypting field values”](#) on page 209.
- How many fields are included in the field group - how many new fields will the new field group contain? If you are creating more than one new field for an object, consider categorizing collections of object field definitions in the same field group for ease of maintenance.
- What is the Display Type for the new field? In the Task Focused UI, the Display Type is defined on the field. In the Standard UI, the Display Type is defined on the profile.
- Object views in the Standard UI - Which view pages will display the new field? Views include Detail, Folder, or List. A custom form or survey can only have a detail view page. For more information, see [“Configure views for objects”](#) on page 322.
- Display order in the Standard UI - Where does the new field appear on a view page? What fields should be listed before or after the new field? If no display order is set, the new field will automatically be displayed at the end of the list of fields. For details, see [“Setting the display order of object types \(Standard UI\)”](#) on page 308.

Example

Suppose you want to add an Owner field to several object types. You can either modify the field group for each object type by adding an **Owner** field, or you can create a generic **Owner** field and field group for all object types and reuse it later if you want to add it to an object.

To simplify the work, follow the generic approach and create a generic field that can be added to any object type.

The new field needs a field group and a generic name. Name the field group **Custom Fields** and the name of the field **Owner**. The field name is important because it is the initial label that appears next to the field

wherever the field displays in the application. If necessary, you can modify the label text at a future time. For details on modifying label text, see the chapter, [Chapter 17, “Localizing text,”](#) on page 559.

The **Owner** field will be used to capture a name, so the data type for this field will be Simple String. Since the **Owner** field is considered important, make it a required field so the user must enter a name into the field before they can save and exit the page. No default value will be set for the field so the field will appear empty.

To complete the planning, there are no other fields to be added to the **Custom Fields** field group (**Owner** is the only field). The new **Owner** field will only be displayed on the detail page of the Business Entity and Issue object types (this also includes the add and edit pages).

You must now determine the display order on the Detail view page for both object types. The default order for new fields is at the end of the display list. For simplicity, place the **Owner** field for both object types after the **Modified By** field on the detail page. Because you are using the Platform schema that is supplied by default, the display order of the **Owner** field will need to be set to 8, which is after the **Modified By** field (which is in position 7) on the Detail view page for both objects.

Now that you have identified all the necessary information, you can begin defining fields and field groups.

Field naming guidelines

To create an object field that you can use in reports, there are several factors to consider when choosing a field name.

Avoid using the object name in the field definition

IBM OpenPages with Watson uses a three- or four-character prefix naming convention when generating the Cognos framework model. When Cognos reports are run, the prefix is converted to the object name in the column headers.

For example, in the supplied field definitions, the OPSS-TestResult field group contains a field named Test Result.

Table 86. Prefix conventions		
This prefix	For this object type's fields	Is displayed in a report column header as this
RI_	SOXRisk	Risk
CN_	SOXControl	Control
TR_	SOXTestResult	Test Result

When the Cognos framework model is generated, the Test Result field is converted to the query item "TR_TEST_RESULT".

When the Cognos report is run, the "TR_TEST_RESULT" field column header displays as "Test Result Test Result" by default.

Limit the field name to 20 characters or fewer

Note:

- Limit the name definition to 20 character or less because characters that exceed 20 are truncated.
- The framework generator reserves character positions 21 and 22 for a unique ID in the query item name. Field names that exceed 20 characters are truncated after the 20th character.
- The object prefix is not counted in these 20 characters.

If are multiple field names are more than 20 character and have no unique characters in the first 20 characters, recreate the Reporting Schema only when necessary. The Cognos Reporting Schema

generator may not generate the same two-digit unique ID for the field definitions for each reporting cycle. Reports that use these field definitions may not clearly identify each field definition.

<i>Table 87. Example of framework generator naming results</i>		
This Reporting Schema generation	For a field definition with this name	May result in this
Generation #1	Total Actual Financial Loss 2008	LE_TOTAL_ACTUAL_FINANCI01
Generation #2	Total Actual Financial Loss 2007	LE_TOTAL_ACTUAL_FINANCI01
Generation #3	Total Actual Financial Loss 2006	LE_TOTAL_ACTUAL_FINANCI01

If a long field definition name is required, create the name with unique characters at the beginning of the name, such as "2008 Total Actual Financial Loss" instead of "Total Actual Financial Loss 2008".

Running the Schema Analysis report

Before adding fields to an object type, run the Schema Analysis report to determine the number of object fields that can be added to an object type.

The report shows how many object fields:

- Are currently configured for an object type
- Can "safely" be added to extend that object type

In general, 350 is the threshold limit for the number of fields that can be added to an object type when the average of all field names is 22 characters in length. By keeping the average field name short, it might be possible to include more than the 350 threshold limit for the number of fields.

Important:

Calculations on the Schema Analysis report use and display 175 as the threshold limit rather than 350. You can add more fields than the report shows.

Additionally, each currency field within an object type equates to six fields. This is because each currency field has six distinct columns within the database RT_ table. These six columns equate to the core currency field and its five subfields: Local Amount, Local Currency Code, Exchange Rate, Base Amount, and Base Currency Code.

The Schema Analysis report is accessed through the IBM Cognos Analytics. The Report lists all object types, in alphabetical order, that are in the schema. The following example shows the name of each column in the Report and sample data for the Control object type.

<i>Table 88. Information in the Schema Analysis report</i>	
Report Column Name	Example
Object type	rt_control
Current number of fields	39
Current Field Length Statistics (Highest/Average)	22/14
Number of Additional Fields that can be added (assuming Maximum Field Lengths are used)	136
Potential Number of Additional Fields that can be added (if the Average Field Length for this Object Type does not increase)	187

For example, you want to add three currency fields to the Control object type. Because each currency field equates to six fields, you would be adding 18 fields to the Control object type (3 X 6).

Using the numbers from the Example column in [Table 88 on page 202](#), the Schema Analysis report indicates that the Control object type (rt_control) in the sample schema currently has 39 fields. Of those 39 fields, the largest field length is 22 characters, with an average field length (for all fields) of 14 characters.

The report also indicates that you can add 136 fields with names that do not exceed 22 characters in length, or up to 187 fields if the field names are 14 characters (or less). Adding the three currency fields (for a total of 18 fields) would be well within the threshold for this object type.

The values 136 and 187 are calculated based on 175 as a threshold limit. Since the threshold is 350, you can actually add approximately 311 or 413 fields, respectively.

Procedure

1. In the Task Focused UI, click **Analytics**.
2. Click **Team content**.
3. On the **Team content** page, navigate through the links as follows:
OpenPages_Platform_V6 > Administrative Reports
4. On the **Administrative Reports** page, click the **Schema Analysis Report** link to run the report.

Data types

The IBM OpenPages with Watson application provides various data types from which you can choose.

After you select a data type for a field and save it, only the parameters or settings for the data type can be modified; you cannot change the data type itself.

To display more parameters for a selected data type when using the Standard UI, click the double arrow icon next to the data type selector.

Boolean data type

A logical operator that has the following predefined values: **true** (default) or **false**.

For more information, see [“Defining boolean fields ” on page 211](#).

Business entity selector data type

A business entity selector data type field displays a business entity structure and allows users to move up and down the structure to locate and select a specific business entity. .

The business entity selector data type is available only in the Task Focused UI.

For more information, see [“Defining business entity selector fields ” on page 211](#).

In the Standard UI, a business entity selector field is defined as a display type for a simple string field. For more information, see [“Configuring the Business Entity Selector display type for simple string fields \(Standard UI\)” on page 350](#).

Classifier data type

The classifier data type accepts simple string text that can be interpreted and classified by a natural language processing service that uses Watson technology.

For more information, see [“Defining a Classifier Configuration \(Task Focused UI\)” on page 1028](#) and [“Defining a classifier field” on page 212](#).

Currency data type

The currency data type accepts numeric values with decimal places for currency values.

For more information, see [“Defining currency fields” on page 212.](#)

Date data type

The date data type default value is blank and this value cannot be changed. The date picker pop-up box defaults to the current date.

For more information, see [“Defining a date field ” on page 215.](#)

Decimal data type

The decimal data type accepts numeric values with decimal places. A value range and default value can optionally be specified. If a user enters a value that is either below or above the specified value range or a non-decimal value, an error message is shown.

For more information, see [“Defining decimal fields” on page 216.](#)

Enumerated String data type

The enumerated string data type accepts a list of string values. Define the values for the list and whether multiple values can be selected. A default value can optionally be specified.

For more information, see [“Defining enumerated string fields” on page 216.](#)

Integer data type

The integer data type accepts numeric values without decimals. A value range and default value can optionally be specified. If a user enters a value that is either below or above the specified value range or a non-integer value, an error message is shown.

For more information, see [“Defining integer fields” on page 217.](#)

Long String data type

A long string is considered to be any text of length more than 4000 bytes. Long strings allow users to enter more than 4000 bytes in a single field.

You can encrypt long string field values up to a maximum of 2 MB in the IBM OpenPages with Watson repository.

The long string data type has the following subtypes:

- Medium

Medium is a fixed size of 32 KB. Medium is the only size that is supported for FastMap uploads.

- Large

Large is a default size of 256 KB. It can be increased by changing the **Platform > Repository > Resource > Large Text > Maximum Size** setting. Enter a value in bytes. The maximum size applies to all large subtype long strings.

Important: After it is set, this value cannot be reduced.

Note: The maximum size is a hidden setting. To show hidden settings set **Applications > Common > Configuration > Show Hidden Settings** to **true**.

The display type determines how a long string field is presented to the user.

In the Task Focused UI, long string fields can have the following display types:

- Rich Text

Provides a text display area with a toolbar and commands for text formatting and word processing.

The toolbar can be minimized or expanded. The space used for non-printing, formatting, and multi-byte

characters might cause the data to exceed the size of the medium long string field, resulting in an error message.

- Text Area

Provides a box display area in which users can enter either plain or HTML-formatted text.

In the Standard UI, long string fields can have other display types. For more information, see [“Configuring display types for simple string fields \(Standard UI\)”](#) on page 349.

- For more information, see [“Defining long string fields”](#) on page 217.
- For more information about filtering on long string fields, see [“Utilities for filtering on long string field content in an Oracle database”](#) on page 746 and [“Utilities for filtering on long string field content in a Db2 database”](#) on page 702.
- For more information about concatenating simple string fields into a long string field, see [“String concatenation utility”](#) on page 752
- For more information about encrypting fields, see [“Configure field level encryption”](#) on page 152.
- For more information about setting display types for long string fields in the Standard UI, see [“Configuring display types for long string fields \(Standard UI\)”](#) on page 358.

Reporting Fragment data type

The Reporting Fragment data type displays a component (such as a bar or line chart) from a Cognos report or dashboard in a field. For more information, see [“Reporting fragment fields”](#) on page 238.

Simple String data type

The simple string data type, by default, displays data as text. The default value of the field is blank. The maximum size of a simple string is 4000 bytes.

You can encrypt simple string field values in the IBM OpenPages with Watson repository. You can also provide a default value.

The display type determines how the field is presented to the user.

In the Task Focused UI, simple string fields can have the following display types:

- Link

Contains a URL value. It validates that the internet address is a fully qualified URL internet address (for example, <http://www.mycompany.com> or <ftp://ftp.myftpsite.com>) and will display an error message to the user if the format of the internet address is incorrect. The Link display type was named URL in the Standard UI.

- Rich Text

Provides a text display area with a toolbar and commands for text formatting and word processing. The toolbar can be minimized or expanded. You may not be able to enter 4000 rich text characters into the text display area because of the space used for formatting and multi-byte characters.

- Text

Provides a box area in which users can enter a string value.

Note: When generating reports in PDF format, rich text fields do not render properly and the format is not preserved.

- Text Area

Provides a box display area in which users can enter either plain or HTML-formatted text.

After it is defined, you cannot change a field defined as simple string data type to long string data type.

For more information, see [“Defining simple string fields”](#) on page 218.

In the Standard UI, simple string fields can have other display types. For more information, see [“Configuring display types for simple string fields \(Standard UI\)”](#) on page 349.

User/Group data type

The User/Group data type allows the selection of users and/or groups. The display type controls whether the field is for users and/or groups and whether single or multiple selections can be made.

A User/Group field can have the following display types:

- Group Selector
Allows the selection of a single user group.
- Multi-valued Group Selector
Allows the selection of multiple user groups.
- Multi-valued User Selector
Allows the selection of multiple users.
- Multi-valued User/Group Selector
Allows the selection of multiple users and/or groups.
- User Selector
Allows the selection of a single user.
- User/Group Selector
Allows the selection of a single user or group.

The following additional settings for user/group fields are defined on the profile:

- Include Disabled
- Starting Group
- Include Subgroups

The User/Group data type is available only in the Task Focused UI. For more information, see [“Defining user/group fields”](#) on page 219.

In the Standard UI, user/group fields are defined as simple string fields with a display type defined on the profile that controls user/group and single/multiple selection. For more information, see [“Configuring display types for simple string fields \(Standard UI\)”](#) on page 349.

Single File data type (Standard UI only)

For legacy internal use. Do not use because this data type cannot be used in profiles.

Defining field groups

A field group is a container for fields. Each field you create must belong to a field group.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode”](#) on page 71.
2. Click  > **Solution Configuration** > **Object Types**.
3. Select an object.
4. Expand the **Fields** section.
5. To create a field group, click **New Field**.
6. Click **New** next to **Field Group**.

7. Enter a **Name** and **Description**
8. Continue defining the new field.
9. Click **Create**.

What to do next

Add field definitions to the new field group. For details, go to [“Defining fields and adding them to field groups” on page 207](#).

Adding field groups to object types

A field group must be assigned to an object type.

About this task

Use this task to assign and unassign field groups to an object type. You can also change a field group description and create new fields.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71](#).
2. Click  > **Solution Configuration** > **Object Types**.
3. Select an object.
4. Expand the **Field Groups** section.

Field groups that are already assigned to the object type are listed.
5. Click **Add Field Groups** to add a field group to the object type.
 - a) In **Field Groups**, select all the field groups to add to the object type.
 - b) In **Add fields to Profiles**, select the profile to add the field group to.
 - c) Click **Done**.
6. Select a field group.
 - a) Change the description, if needed.
 - b) Click **New Field** to create a field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).
 - c) Click **Done**.

Defining fields and adding them to field groups

A field definition stores the data type and other properties of a field.

For each new field to add to an object type, you must create a field definition that defines the properties of that field. You can add a field definition to an existing field group or create a new field group.

Before you begin

Learn about data types and display types. For more information, see [“Data types” on page 203](#).

If the field group is already associated to an object type and you use IBM Db2 and the reporting schema is enabled, perform this task when there is limited or no activity on the system. It can cause significant system delays in OpenPages due to locking conflicts on the Db2 platform. For more information, see [“System delay when modifying object types and fields \(Db2\)” on page 1107](#).

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode”](#) on page 71.
2. Click  > **Solution Configuration** > **Object Types**.
3. Click an object type.
4. Expand the **Fields** section to work with fields and field groups.
5. Click **New Field**.
6. In **Field Group**, select the field group that the new field is assigned to.
Or, click **New** to create a new field group. Enter a **Name** and **Description** and click **Create**.
7. Enter a **Name**. The name must start with a letter, and can contain only letters, numbers, spaces, and the underscore (_) character. After it is defined, you cannot change a field's name. You can, however, change the label.
8. Enter a **Label**. Click **Edit** to add values in multiple languages.
9. Enter a **Description**.
10. Select a **Data Type** and complete the fields that are specific to that data type.

Table 89. Data Types	
For this data type...	See this topic...
Boolean	“Defining boolean fields ” on page 211
Business Entity Selector (Task Focused UI only)	“Defining business entity selector fields ” on page 211
Classifier	“Defining a classifier field” on page 212
Currency	“Defining currency fields” on page 212
Date	“Defining a date field ” on page 215
Decimal	“Defining decimal fields” on page 216
Enumerated String	“Defining enumerated string fields” on page 216
Integer	“Defining integer fields” on page 217
Long String	“Defining long string fields” on page 217
Reporting Fragment	“Reporting fragment fields” on page 238
Simple String	“Defining simple string fields” on page 218
User/Group (Task Focused UI only)	“Defining user/group fields” on page 219

11. Set **Required** to True or False. For more information, see [“Making fields required or optional”](#) on page 209.
12. Set **Global Search** to True or False.

Fields that are encrypted are not eligible for use in Global Search.



CAUTION:

Enabling Global Search for simple or long string fields that have field level security might result in users being able to derive data values they otherwise would not have access to. For more information, see [“Field level security”](#) on page 133.

13. In **Profiles**, assign the field to one or more profiles. By default, all profiles that the object type belongs to are selected.

14. Click **Create**.
15. Add more fields to the field group, as needed.
16. To edit a field, click a field row.
 - a) Edit settings on the field. Click **Edit** next to **Label** to update label values. Description can also be edited. Not all fields can be changed, for example, the **Name** cannot be changed. The settings that are displayed depend on the field type.
 - b) Expand **Profiles**. View and change the profile that the field is assigned to.
 - c) Click **Done**.

Making fields required or optional

You can globally set whether or not all users are required to enter data in an object field.

When you create a new object field, by default, the **Required** setting is False, which means the field is optional or non-required during data entry.

Note: If you want to require a specific group of users (not all users) to enter data for a field, for maximum flexibility set the field as required in the profile and not in the field definition (see [“Setting a field in a profile to required or optional”](#) on page 307).

When you set an object field to be required, a red asterisk * displays after the field label. For example, if you were to change the setting of the optional "Additional Description:" field of the Account object to be a required data entry field, it displays to users as "Additional Description*:" Users are required to enter information in the field when they created a new Account object.

You can omit a required field for a particular view if the field is filled in by a trigger or if the field will have been filled in prior to this view being used to edit the object.

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups”](#) on page 207.
2. Set **Required**:
 - True - the field is required
 - False - the field is optional
3. Finish defining the field. For more information, see [“Defining fields and adding them to field groups”](#) on page 207.

What to do next

Note: Changing a field to Required also causes all profile references to the field to be required as well.

Encrypting field values

You can encrypt a simple string or long string field value in the IBM OpenPages with Watson repository to prevent system administrators from viewing confidential data directly from the database. Encrypted field values are shown as a string of random characters.

Note: Before encrypting long strings in OpenPages running on Oracle 12.2, refer to the following Technote: <http://www.ibm.com/support/docview.wss?uid=swg22010106>. The Technote describes a potential issue and how to resolve it by obtaining the appropriate patch from Oracle support and applying it to your environment.

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).
2. To encrypt all values for the field, set **Encrypted** to True.
3. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).

Results

The field is now marked for encryption. The timing of the encryption depends on the status of the field level encryption keystore:

- If keystore is enabled, all field values are encrypted when you save the field definition.
- If the keystore is disabled, no field values are encrypted until you enable the keystore.

For more information, see [“Configure field level encryption” on page 152](#).

Decrypting field values

You can decrypt a simple string or long string field value in the IBM OpenPages with Watson repository if the data is no longer considered to be confidential. System administrators can view decrypted data directly from the database.

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).
2. To decrypt all values for the field, set **Encrypted** to False.
3. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).

Results

The field is now marked for decryption. The timing of the decryption depends on the status of the field level encryption keystore:

- If the keystore is enabled, no field values are decrypted until you disable the keystore.
- If keystore is disabled, all field values are decrypted when you save the field definition.

For more information, see [“Configure field level encryption” on page 152](#).

Setting a default value for an object field

When you create a new object field, by default, the **Default Value** property is empty (not populated).

When you set a default value for an object field, that value displays to users in that field. For example, if you were to set a default value for the "Additional Description:" field of the Account object that contained the text "Enter any additional information here.", it displays to users when they created a new Account object.

Restriction: The new default value will only be populated for new instances of an object type. In other words, if a user attempts to edit an existing object where the value was blank, it will remain blank. The new default value will be used when a user or administrator creates a new instance of that object type. For example, if an administrator modifies an enumerated string (dropdown field) on a test object. The new default value will be populated if new test objects are created. If an end user attempts to edit an existing test object, the new default value won't be set or modified for it.

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).
2. In **Default Value**, either type a value, make a selection, or selected enumerated string values.
3. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).

Defining boolean fields

Define a boolean field by setting the data type and a default value.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 203](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).
2. Select Boolean in **Data Type**.
3. Select True or False in **Default Value**.
4. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).

Defining business entity selector fields

Define a business entity selector field by setting the data type and additional settings on profiles.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 203](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).
2. Select Business Entity Selector in **Data Type**.
3. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).

What to do next

Click  > **Solution Configuration** > **Profiles**. Select a profile to modify and a business entity selector field. Set the following values:

Table 90. Business Entity Selector options on profiles	
Setting	Description
Starting Business Entity	The default value for Starting Business Entity is a forward slash (/). If you want all Level 1 business entities displayed, retain the default. To set a starting business entity, navigate through the business entity tree and select a business entity.

Table 90. Business Entity Selector options on profiles (continued)

Setting	Description
Number of Levels	Determines the number of levels that end users can navigate to from the starting business entity. For example, if you select Global Financial Services as your starting business entity and set the number of levels to 2, you can navigate to two levels below Global Financial Services (Global Financial Services/Asia Pac/Agency Services). Limit the number of levels to improve performance of the selector and help users select from the entities most appropriate for this field. The default value is 3.

Defining a classifier field

Define a classifier field by setting the data type and additional settings.

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups”](#) on page 207.
2. Select Classifier in **Data Type**.
3. Enter a **Classifier Configuration Name**. The name of a classifier configuration defined in  > **Integrations > Mapping and Taxonomy Suggestions**.
Or, in 8.2.0.3 and earlier,  > **Watson Integrations > Mapping and Taxonomy Suggestions**.
4. Select a **Classifier Input Field**. The field that provides text that is interpreted and classified by a natural language processing service. In the Standard UI, use the format <Field Group>.<Field Name>
5. Finish defining the field. For more information, see [“Defining fields and adding them to field groups”](#) on page 207.

Defining currency fields

Define a currency field by setting the data type, Include Conversion, a value range, and defining additional settings on profiles.

Before you begin

Learn about the data type. For more information, see [“Data types”](#) on page 203.

About this task

- The Minimum Value and Maximum Value settings are expressed in terms of the base currency (base currency is set during installation). If a user enters a value that is either below or above the value range, an error message is shown.
- You cannot use non-numeric characters when you enter currency values. For example, either 125000 or 125,000 is legal, but not \$125000. This format is set per user locale.
- Object fields with this data type cannot be included in the profile of predefined objects or custom forms that use the supplied JSP file for rendering.

Note: The Currency data type does not support computed fields. See [“Defining a computed field”](#) on page 227 for information on computed fields.

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 207.](#)
2. Select Currency in **Data Type**.
3. Set **Include Conversion** to True or False to control whether the exchange rate and base amount conversion are visible.
 - **True** (default) - the following items are displayed to the user when they work with the currency field:
Local Currency Code (drop down)
Local Amount (text input)
Exchange Rate (text input)
Base Code (static text)
Base Amount (static text)

For example, you might use this setting when the field represents a currency amount relative to a specific point in time where the exchange rate is applicable, such as a financial loss on a specific date.
 - **False** - the following items are displayed to the user when they work with the currency field:
Local Currency Code (drop down)
Local Amount (text input)

For example, you might use this setting when the field represents a hypothetical currency amount not relative to a specific point in time, such as Inherent Severity on the Risk object.
4. Optional: In **Minimum Value** enter the lowest value that is allowed.
5. Optional: In **Maximum Value** enter the greatest value that is allowed.
6. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 207.](#)

What to do next

Click  > **Solution Configuration** > **Profiles**. Select a profile to modify and a currency field. Set the following value:

Table 91. Currency field settings on profiles	
Setting	Description
Exchange Rate Read Only	Controls whether exchange rates for the currency are read only. If the Exchange Rate Read Only value is set to: • True - exchange rates for the currency are read only • False - exchange rates for the currency are not read only

Modifying currency exchange rates

You can add, edit, enable, and disable currency exchange rates.

Currency exchange rates can be accessed using tasks in either the Task Focused UI or the Standard UI. Changes made in one interface are immediately reflected in the other.

From either access point, you need the **SOX > Administration > Currencies** application permission.

Use one of the following methods to update currency exchange rates.

- Upload a CSV file with currency exchange rates from:
 - The **Currencies** task in the Task Focused UI. For more information, see [“Editing, enabling, disabling, and uploading currency exchange rates \(Task Focused UI\)”](#) on page 215.
 - The **Administration > Currencies** task in the Standard UI. For more information, see [“Uploading a CSV file \(Standard UI\)”](#) on page 237.
 - An ObjectManager loader file. For more information, see [“Importing exchange rates”](#) on page 902.
- Edit the rates manually in the Task Focused UI. For more information, see [“Editing, enabling, disabling, and uploading currency exchange rates \(Task Focused UI\)”](#) on page 215.
- Edit the rates manually in the Standard UI. For more information, see [“Editing exchange rates for an existing currency code \(Standard UI\)”](#) on page 237.
- Upload currency exchange rates in an ObjectManager loader file. For more information, see [“Importing exchange rates”](#) on page 902.

Note: You cannot use these functions with a new currency. The currency must exist.

Formatting a CSV file

The file containing the exchange rate currency data must be in a comma separated value (.csv) file that is formatted in a specific way.

The file must have the following format:

```
<currency code>,<exchange rate>
<currency code>,<exchange rate>
```

Where:

Table 92. CSV file format placeholders for exchange rates	
Field	Description
<currency code>	The 3-letter ISO Currency Code.
<exchange rate>	The numeric exchange rate value. The default value is 1.0.
<start date>	Optional. The date the exchange rate was (or will be) applied. You can use either of the following formats: • mm/dd/yyyy • mm/dd/yyyy HH:mm:sss If no historic date is supplied, the current date is used.

The following data sample from a CSV file shows the ISO currency codes for Euros, Canadian dollars, and Japanese yen with the corresponding exchange rate for each currency, and the historical date that the rate was applied for two of the three currencies.

```
EUR,0.1589,12/26/2007
CAD,0.8636
JPY,0.0083,5/8/2008
```

The number of rows in the CSV file might be limited. For more information, see [“Maximum rows in exchange rate upload file”](#) on page 635.

Editing, enabling, disabling, and uploading currency exchange rates (Task Focused UI)

You can edit, enable, and disable currency exchange rates. You can also upload exchange rates from a CSV file.

Before you begin

To upload exchange rates, create the CSV file. For more information, see [“Formatting a CSV file” on page 214](#).

About this task

You can enable disabled currency rates, making them available to the appropriate processes.

You can disable enabled currencies. When you disable a currency it is no longer available to the system. However, it is not deleted. You can enable it at any time.

Note: You cannot enable or disable the base currency, which is set during installation.

Procedure

1. Click  > **System Configuration** > **Currencies**.
2. To view a currency and its exchange rates, select it.
3. To upload a CSV file, deselect all currencies and click **Upload**. Select a file and click **Upload**.
The new currency exchange rate appears in the list of enabled currencies.
4. To manually edit the exchange rates for one or more currencies, deselect all currencies and click **Edit**. Edit the exchange rates and click **Save**. For each change, a new exchange rate with today's timestamp is created.
5. To enable a currency, deselect all currencies and click **Enable**. All currencies are listed. Select the currencies that you want to enable and click **Enable**.
The currency appears in the list of enabled currencies.
6. To disable a currency, select it and click **Disable**.
The currency is no longer shown in the list of enabled currencies.

Defining a date field

Define a date field by setting the data type.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 203](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).
2. Select Date in **Data Type**.
3. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).

Defining decimal fields

Define a decimal field by setting the data type, a value range, and a default value.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 203](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).
2. Select Decimal in **Data Type**.
3. Optional: In **Minimum Value** enter the lowest decimal value that is allowed.
4. Optional: In **Maximum Value** enter the greatest decimal value that is allowed.
5. Optional: In **Default Value** enter a numeric value that is between the minimum and maximum allowable values.
6. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).

Defining enumerated string fields

Define an enumerated string field by setting the data type, adding values, and defining whether it is encrypted and single or multi-valued. A default value can also be specified.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 203](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).
2. Select Enumerated String in **Data Type**.
3. Set **Multi Valued**:
 - True - multiple values can be selected from the list.
 - False - only one value can be selected from the list (the default).
4. Add values to the list:
 - a) In **Enumerated String Values** click **New Value**.
 - b) Enter a **Name**.
 - c) Click **Create**.
5. To reorder the values in the list, use drag and drop and position the values in the correct display order.
6. Hover over a value and click the show/hide icon to control whether a value is displayed to users.
7. To remove a value from the list, click the remove icon next to the value.
8. Optional: In **Default Value** select a value that is the default.
9. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).

Results

After an enumerated field, either single or multi-valued, is created, a true/false toggle named **Hierarchical** might be displayed. It is an internal setting and cannot be changed.

In the Standard UI:

- To reorder the list of values, see [“Changing the order of enumerated string values \(Standard UI\)”](#) on page 233.
- To set the display of the enumerated string data, such as a list, radio buttons, or check boxes, you must do it through the profile, see [“Configuring a display type for enumerated strings \(Standard UI\)”](#) on page 361.

After it is defined, you cannot change an enumerated string field from a multi-value enumerated string data type to single-value enumerated data type.

If you are using Oracle, you can convert a single value selection setting to a multi-value selection setting.

If you are using IBM Db2 and you want to convert a single value selection setting to a multi-value selection setting, you must:

- Perform the conversion when there is limited or no activity on the system if the reporting schema is enabled. The conversion can cause significant system delays in OpenPages due to locking conflicts on the Db2 platform. For more information, see [“System delay when modifying object types and fields \(Db2\)”](#) on page 1107.
- Complete remediation steps after the conversion is finished. For more information, see [“Remediating after an Enumerated String field is changed to a multi-select field \(Db2\)”](#) on page 1106. Or, drop the reporting schema, change the setting, and then recreate the reporting schema.

Defining integer fields

Define an integer field by setting the data type, a value range, and a default value.

Before you begin

Learn about the data type. For more information, see [“Data types”](#) on page 203.

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups”](#) on page 207.
2. Select Integer in **Data Type**.
3. Optional: In **Minimum Value** enter the lowest integer value that is allowed.
4. Optional: In **Maximum Value** enter the greatest integer value that is allowed.
5. Optional: In **Default Value** enter an integer value that is between the minimum and maximum allowable values.
6. Finish defining the field. For more information, see [“Defining fields and adding them to field groups”](#) on page 207.

Defining long string fields

Define a long string field by setting the data type, string size, display type, encryption, and providing a default value.

Before you begin

Learn about the data type. For more information, see [“Data types”](#) on page 203.

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups”](#) on page 207.
2. Select Long String in **Data Type**.
3. Select a **String Size**:
 - Medium

- Long
4. Select a **Display Type**:
 - Rich Text
 - Text Area
 5. Set **Encrypted** to True or False.

Long string fields that are encrypted:

 - are not eligible for use in Global Search.
 - display a blank result when used as filter criteria.

For more information, see [“Encrypting field values” on page 209](#) and [“Decrypting field values” on page 210](#).
 6. Enter a **Default Value**. Type a string of either plain text or HTML-formatted text.

For more information, see [“Setting a default value for an object field” on page 210](#).
 7. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).

Defining simple string fields

Define a simple string field by setting the data type, string size, display type, encryption, and providing a default value.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 203](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).
2. Select Simple String in **Data Type**.
3. Select a **Display Type**.

Valid values for simple strings are:

 - Link
 - Rich Text
 - Text
 - Text Area
 - Show full list of display types

Do not create new fields with the Show full list of display types option. Use this option only for imported fields that have no display type. This can happen if a field is imported that did not have an assigned profile in the same configuration file.
4. Set **Encrypted** to True or False.

Simple string fields that are encrypted:

 - are not eligible for use in Global Search.
 - cannot be defined to use security rules (both record level and field level). For more information, see [“Security rules” on page 120](#).

For more information, see [“Encrypting field values” on page 209](#) and [“Decrypting field values” on page 210](#).
5. Enter a **Default Value**. Type a string of either plain text or HTML-formatted text.

For more information, see [“Setting a default value for an object field” on page 210](#).

6. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).

Defining user/group fields

Define a user/group field by setting the data type, display type, and defining additional settings on profiles.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 203](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).
2. Select User/Group in **Data Type**.
3. Select a **Display Type**.
Valid values for user/group fields are:
 - Group Selector
Allows the selection of a single user group.
 - Multi-valued Group Selector
Allows the selection of multiple user groups.
 - Multi-valued User Selector
Allows the selection of multiple users.
 - Multi-valued User/Group Selector
Allows the selection of multiple users and/or groups.
 - User Selector
Allows the selection of a single user.
 - User/Group Selector
Allows the selection of a single user or group.
4. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 207](#).

What to do next

Improve the performance of user/group fields by setting additional fields on profiles.

If your deployment has a large number of users, the performance of the User Selector or the Multi-Valued User Selector in opening and loading data may be sluggish. One way to improve the performance of the User Selector or the Multi-Valued User Selector is to configure it so it only retrieves users that have permission on the object being edited. You do this by setting **Minimum Access** on profiles.

The supplied profiles in the IBM OpenPages with Watson application are configured such that the User Selector or Multi-Valued User Selector pop-up retrieves all users in the system - including some application users who do not have security permissions on the selected object. This might result in the assignment of a user as "owner" on an object when the user does not have read access on the object.

Set **Minimum Access** to restrict the set of users retrieved by the User Selector or the Multi-Valued User Selector to those users that have access permissions on the object being edited at the time.

Click  > **Solution Configuration** > **Profiles**. Select a profile to modify and a user/group field. Set the following values:

Table 93. Additional selector settings

Setting	Description
Include Disabled	Allows or disallows disabled user accounts to be included in a selector listing. If the Include Disabled value is set to: • True - disabled user accounts are included in the selector listing. When this setting is selected, the Minimum Access setting is disabled. A value of True, when used in combination with a Starting Group value that contains many users, can result in slower search performance. • False - disabled user accounts are excluded from the selector listing. When this setting is selected, the Minimum Access setting is enabled. This setting generally applies to User (not Group) selectors.
Starting Group	Controls which group displays at the beginning of the selection hierarchy. If the Starting Group value is blank, selectors search the system for all users and/or groups, depending on the display type. A blank Starting Group value used in combination with an Include Disabled value of True can result in improved search performance. To select a starting group, click the group icon and select a valid group name from the selector window. For example, if you are using role-based security, you could select the Security Domains group, for non role-based security, you could select the Workflow, Reporting and Others group.
Include Subgroups	Controls whether subgroups are included or excluded from the User selector listing. Note: This setting applies only to the User/Group and Group selectors. If the Include Subgroups value is set to: • True - subgroups are included in the selector listing. • False - subgroups are excluded from the selector listing.

Table 93. Additional selector settings (continued)

Setting	Description
Minimum Access • Read • Write • Delete • Associate	This setting is enabled only if the Include Disabled value is set to False. This setting allows you to filter users based on access control list settings on an object's folder. For example, you want to limit the number of users who can be assigned as a Process "Cycle Owner", which is an object field with a user selector display type for the Process object. Because you previously set up an access control list (ACL) for one or more groups or users to the Process folder, you can use the Minimum Access setting to filter the list of users. If you only wanted users with "Delete" permissions to be displayed on the user selector list, you can select the "Delete" Minimum Access setting to filter and display only those users with "Delete" ACL permissions. If the Read box is: • Selected - only users with Read access are displayed on the user list. • Cleared - no filtering occurs. If the Write box is: • Selected - only users with Write access are displayed on the user list. • Cleared - no filtering occurs. If the Delete box is: • Selected - only users with Delete access are displayed on the user list. • Cleared - no filtering occurs. If the Associate box is: • Selected - only users with Associate access are displayed on the user list. • Cleared - no filtering occurs.

Field and field group process overview (Standard UI)

You can add new fields to an object type and then display the new fields.

Fields can be object fields, computed fields, and report fragment fields.

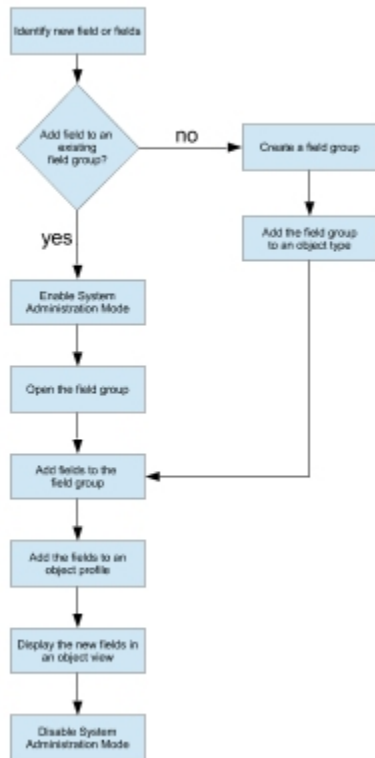


Figure 13. Tasks for configuring new fields

Table 94 on page 222 provides information about the configuration tasks.

Table 94. Tasks for configuring new fields	
Task Description	Related Topic
1. Identify the new field.	See “Requirements for new fields” on page 200 for the information to identify before you create a new field.
2. Add a new field group or identify the existing group where the field is associated.	See “Adding field groups (Standard UI)” on page 223 for instructions on how to create a new field group.
3. Add field definitions to the field group.	See “Adding fields to a field group (Standard UI)” on page 223 for instructions on how to add new field definitions to a new field group.
4. If you created a new field group, add it to the appropriate object type.	See “Including field groups for an object type (Standard UI)” on page 255 for information about how to add the new field group to an object type or custom form object type.
5. Display the new fields in an object view.	See “Configure views for objects” on page 322 for information on displaying the new fields in a selected view and configuring a display type.

Adding field groups (Standard UI)

A field group is a container for fields. Each field you create must belong to a field group.

Procedure

1. Enable System Administration Mode.
2. Click **Administration > Field Groups**.
3. On the **Field Groups** table, click **Add**.
4. On the **Field Groups** page, type a name for the field group.
5. Click **Create**.

What to do next

Add field definitions to the new field group. For details, go to [“Defining fields and adding them to field groups”](#) on page 207.

Adding fields to a field group (Standard UI)

A field group can contain one or more fields.

A field definition stores the data type and other properties of a field. For each new field to add to an object type, you must create a field definition that defines the properties of that field. You can add a field definition to a new field group or an existing field group that is not in use.

Before you begin

If the field group is already associated to an object type and you use IBM Db2 and the reporting schema is enabled, perform this task when there is limited or no activity on the system. It can cause significant system delays in OpenPages due to locking conflicts on the Db2 platform. For more information, see [“System delay when modifying object types and fields \(Db2\)”](#) on page 1107.

Procedure

1. Enable System Administration Mode.
2. Click **Administration > Field Groups**.
3. In the **Field Definitions** table of the field group, click **Add**.
4. On the **Field Definition** page, type a name and select a data type.

The following table lists the properties that you can specify:

Table 95. Field definition properties	
In this box...	Do this...
Name	Type a name for the field. Important: The name must start with a letter, and can contain only letters, numbers, spaces, and the underscore (_) character. Examples: Owner, owner1, Owner1_Risk After it is defined, you cannot change a field's name. You can, however, change the label.
Description	Type a description of the field.

Table 95. Field definition properties (continued)	
In this box...	Do this...
Data Type	Select a data type for this field: - Click the down arrow and select a data type from the list. - Click the double arrows (>>) to display more options for the selected data type. For details see, “Data types” on page 203.
Computed Note: This additional option appears for most data types.	Select this box if you want this field to be a computed field. More boxes are displayed. For details, see, “Creating computed fields (Standard UI)” on page 225.
Required Note: This additional option appears for all data types.	Select this property if you want the field to require data entry. For details, see, “Making fields required or optional” on page 209.

- Click **Create**. The new field definition is listed on the Field Definitions table of the selected field group.
- To add another field definition to this field group, repeat Steps 2, 3, and 4.
- When finished adding field definitions, add the field group to one or more object types. For details, go to [“Including field groups for an object type \(Standard UI\)” on page 255.](#)

Modifying field group properties (Standard UI)

You can modify the description property of any field group; however, the name of a field group cannot be changed.

Procedure

- Click **Administration > Field Groups**.
- Click the name of the field group that you want to modify to open its details page.
- On the **Field Group Information** table, click **Edit**.
- Modify the description as necessary.
- Click **Save**.

Modifying object field definitions (Standard UI)

After you create an object field, you can modify field definition properties.

For any type of object field - modify the description, whether the field is required or optional, and set a default value for the field (excluding the Date data type). For numeric fields, such as decimal or integer, change the minimum, maximum, and default values.

For fields with enumerated strings, you can add, delete (if not in use), hide or unhide, and update the order of the values in the list. For more information, see [“Adding enumerated string values \(Standard UI\)” on page 232](#)

Note: You cannot modify the name of any object field or its data type.

Procedure

- Click **Administration > Field Groups**.

2. Click the name of the field group containing the object field to modify.
3. On the **Field Definitions** table, click the name of the field to modify.
4. On the **Field Definition Information** table, click **Edit**.
5. To define object fields as required or optional, see [“Making fields required or optional” on page 209](#).
6. To set a default value for an object field, see [“Setting a default value for an object field” on page 210](#).
7. Click **Save**.

Deleting field groups (Standard UI)

If a field group has never been associated with an object type (that is, it has never been used), you can then delete it.

When you delete a field group, the field group is removed from the list of available field groups on the **Field Groups** page and cannot be restored to the list.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71](#).
2. Click **Administration > Field Groups**.
3. Select the box next to the name of the field group to delete.
4. Click **Delete** on the **Field Groups** pane.

Deleting an object field definition (Standard UI)

When you delete a field, the definition of the field is removed from the field group to which it belongs.

You can only delete field definitions from a field group that are not in use. After a field definition is deleted, it cannot be restored.

Procedure

1. Access the **Field Groups** page (see [“Adding field groups \(Standard UI\)” on page 223](#)).
2. Click the name of the field group you want to modify to open its details page.
3. Click the box next to the name of each field definition you want to delete.
4. Click **Delete**.

Creating computed fields (Standard UI)

You can create, edit, or view an object field whose value is computed from the values of other fields. These computed fields can exist on either the same object or on another, related object.

Computed fields have the following characteristics:

- Can be defined only in the Standard UI.
- Can be viewed in the Task Focused UI.
- Are always read-only.
- Can be used in reports.
- Can be added to the Context, Detail, Activity, List, Home Page Filtered List, Filtered List, Grid and Folder views in the IBM OpenPages with Watson user interface.
- Must have unique field names. Adding more than one computed field with the same field name in the same view will result in an error.

If you want to import (load) and export (dump) computed field definitions, you must use the ObjectManager tool. For details, see [“Importing computed field definitions” on page 905](#).

Computed fields require an installed and active Cognos server as they use the Cognos Computation Handler. If a computed field is executed in the application and the Cognos server is not available, the following message is displayed to users: *Cognos is unavailable. Please contact your System Administrator.*

Procedure

1. In IBM Cognos Analytics - Reporting, model the computed field in a calculation object. For details, see [“Modeling a new computed field in Cognos” on page 226](#).
2. In the OpenPages with Watson application user interface:
 - a) Define the computed field. For details, see [“Defining a computed field” on page 227](#).
 - b) Regenerate the reporting framework. For details, see [“Updating the reporting framework \(Standard UI\)” on page 978](#).

Modeling a new computed field in Cognos

You can model an equation in Cognos to define a computed field in the application.

Note: If you do not know how to use IBM Cognos Analytics - Reporting, contact an experienced Cognos report author or IBM OpenPages Support.

Procedure

1. Log on to the IBM Cognos Analytics as an IBM OpenPages with Watson user with the locale set to **Report Design Language**.
2. Create a list report that you can use to model the computed field equation.
3. Drag the following ID query items onto the report page to establish a context for the calculation:

- An object ID

Example

```
SOXBUSENTITY HIERARCHY >> SOXPROCESS-SOXCONTROBJECTIVE HIERARCHY  
>> [SOXRISK] >> [RI_RISK_ID]
```

- A reporting period ID

Example

```
SOXBUSENTITY HIERARCHY >> SOXPROCESS-SOXCONTROBJECTIVE HIERARCHY  
>> [SOXRISK] >> [REPORTING_PERIOD_ID]
```

4. Click **Toolbox** on the Insertable Objects pane and complete the following actions:
 - a) Drag a **Calculation** object onto the report page.
 - b) At the prompt, type a name.
For example, type Calc-Risk.
5. In the **Expression Definition** pane of the model, complete the following actions:
 - a) Enter an expression using model query items from the same namespace, function, or parameters.

The Cognos SQL used to define this computed value can be an existing query item in the published Cognos framework or an equation involving multiple query items. Some of the predefined database functions may also be useful for computed fields (such as getting an exchange rate or localizing strings). For details, see the *IBM OpenPages with Watson Report Author's Guide*.

For example, the following equation returns a value with the percentage by which the inherent severity of a risk was reduced after associated controls were applied to that risk. Sample output might be: 2.46.

```
total ([DEFAULT].[SOXCONTROL].[CN_INHERENT_SEVERITY_REDU]
for [DEFAULT].[SOXCONTROL].[RISK_ID]) / 100
```

- b) Validate the expression and make any needed changes.
6. Run the report. Check the results.
7. Click **XML Show Specification** on the toolbar to view the Cognos SQL in an XML representation. The following XML sample shows which sections of the report will be used to define the computed field in IBM OpenPages with Watson and the corresponding field name in the application.

```
<querySet xml:lang="en-ca">
  <BIQuery name="Query1">
    <cube>
      <factList>
        <item refItem="RI_RISK_ID" aggregate="none"/>
        <item refItem="REPORTING_PERIOD_ID" aggregate="none"/>
        <item refItem="Calc-Risk" aggregate="none"/>
      <tabularModel>
        <dataItem name="RI_RISK_ID">
          <expression>[DEFAULT].[SOXRISK].[RI_RISK_ID]</expression>
        </dataItem>
        <dataItem name="REPORTING_PERIOD_ID">
          <expression>[DEFAULT].[SOXRISK].[REPORTING_PERIOD_ID]</expression>
        </dataItem>
        <dataItem name="Calc-Risk">
          <expression>total ([DEFAULT].[SOXCONTROL].[CN_INHERENT_SEVERITY_REDU]
for [DEFAULT].[SOXCONTROL].[RISK_ID]) / 100</expression>
        </dataItem>
      </tabularModel>
    </cube>
  </BIQuery>
</querySet>
```

Note: Because the values in the Report Specification XML window cannot be selected, you can copy the report specification to the Clipboard (**Tools | Copy Report to Clipboard**) and then paste the information into a text document. Then, you can copy the attribute values into the application user interface. The value to be used in the **Equation** definition box can also be obtained from the **Expression Definition** pane of the calculation object.

What to do next

In OpenPages with Watson, define the computed field. For more information, see [“Defining a computed field” on page 227](#).

Defining a computed field

You can define a computed field.

Note: The following data types do not support computed fields: Currency, Enumerated String, and Single File.

About this task

Once you define a field as a computed field, you cannot undo it.

Procedure

1. Click **Administration > Field Groups**.
2. Click the name of the field group in which you want to include the new object field.
3. On the **Field Definitions** table, click **Add**.
4. In the **Name** box, type a name for the new computed field.

5. In the **Description** box, optionally type some descriptive text.
6. Click the **Data Type** arrow and use [Table 96 on page 228](#) to select a data type for the new computed field.

<i>Table 96. Data types for computed fields</i>		
Data Type	Return Value	When to Use
Boolean	TRUE or FALSE (case insensitive)	Takes a boolean string, parses it, localizes it, and displays it.
Date	Date in the format: yyyy-MM-dd'T'hh:mm:ss	Takes a date string, parses it, localizes it, and displays it.
Decimal	Any numbers	Takes any number string and parses it, localizes it, and displays it.
Integer	Whole numbers	Takes a whole number string and parses it, localizes it, and displays it.
Simple String	Any	Can be used for any computed field. Takes the result of the computation engine and displays it. This will not be localized - it displays the exact output of the computation.

If the field is any other data type, use the Simple String data type.

7. Click the double arrow icon  next to the selected data type to display additional parameters.
8. Select the **Computed** option to make the new field a computed field.

When you select **Computed**, the **Required** option disappears and the Cognos Computation Handler attribute fields appear.

If you modeled the computed field in IBM Cognos Analytics - Reporting, the values displayed in the Report Specification XML window are not selectable (see “Modeling a new computed field in Cognos” on page 226). You can copy the report specification to the Clipboard (**Tools | Copy Report to Clipboard**) and then paste the information into a text document where you can then copy the attribute values into the application user interface. The value to be used in the application's **Equation** definition box can also be obtained from the **Expression Definition** pane of the calculation object.

9. Enter a value in the **Equation** box. The equation is the Cognos SQL used to define the computed value for the object field. It can be a reference to an existing query item in the published Cognos framework or an equation involving multiple query items.

For example,

```
total ([DEFAULT].[SOXCONTROL].[CN_INHERENT_SEVERITY_REDU] for
[DEFAULT].[SOXCONTROL].[RISK_ID]) / 100
```

10. Enter a value in the **Primary Namespace** box. The Primary Namespace is the Cognos framework namespace in which the computation is to be performed.

Note: All referenced query items in the values for Equation, Object ID Column, and Reporting Period ID Column must be in the same namespace.

For example, DEFAULT.

11. Enter a value in the **Alternate Namespaces** box if necessary.

The Alternate Namespace is the Cognos framework namespaces to which the computation will be added during reporting framework generation.

Note: See [“Using computed fields with multiple namespaces”](#) on page 229 for an explanation of why a computed field might need alternate namespaces.

12. Enter a value in the **Object Id Column** box. The Object ID Column is a reference to a Cognos framework query item that contains the Resource ID of the computed field's object type. This value must be the same for all computed fields in a given namespace for an object type.

Example: [DEFAULT].[SOXRISK].[RI_RISK_ID]

13. Enter a value in the **Reporting Period Id Column** box. The Reporting Period ID Column is the Cognos framework query item that contains the Reporting Period Id of the computed field's object type. This value must be the same for all computed fields in a given namespace for an object type.

Important: The Resource ID and Reporting Period ID must match within the field group and object type. If these values do not match, the validation will fail.

For example, [DEFAULT].[SOXRISK].[REPORTING_PERIOD_ID]

14. Enter the package label of the reporting package that the field is run against in **Package Name**. The value is case sensitive. The package label for a framework model is defined in the **Platform > Reporting Framework V6 > Models > [model name] > Package Label** setting. If **Package Name** is empty, the package for the OPENPAGES_FRAMEWORK_V6 framework model is used.
15. Click **Create**. IBM OpenPages with Watson will then validate the equation against the primary and alternate namespaces.
16. Regenerate the reporting framework to make the computed field available to report authors. For details, see [“Updating the reporting framework \(Standard UI\)”](#) on page 978.

Using computed fields with multiple namespaces

The IBM OpenPages with Watson application allows multiple parent object types for a given child object type.

The Cognos reporting engine cannot support objects with multiple parent's object types.

For example, in the DEFAULT namespace the only path to a Loss Event is through a Business Entity. This means that if a Loss Event is associated to a parent Risk but not a parent Business Entity, that Loss Event will not be displayed as a result in queries against that namespace. Each parent-child object type relationship that is not contained in DEFAULT is contained in its own namespace.

In order to make the calculation available in multiple namespaces for report writers, you can use the "Additional Namespaces" attribute. This is a comma-delimited list of alternate namespaces for which a "Calculation" object should be created during the framework generation process. During this process, a calculation object is first created for the primary namespace using the value from the "Equation" attribute. Then it creates other calculation objects in other namespaces by taking the equation and substituting the alternate namespaces for the primary namespace.

Note: While an equation may be valid in one namespace, it may not be valid in others. While in most cases this is not a problem, if the query subject name or query item name varies across namespaces you may need to create separate computed field instances with different equations.

Nesting computed fields

Computed fields can sometimes act as building blocks for other computed fields.

These are referred to as intermediate computations. Currently the IBM OpenPages with Watson application does not support intermediate calculation definitions through the IBM OpenPages with Watson user interface. If you want to reference another computed field, you must replicate the equation used in that computed field inside the equation for the current field.

For example, if we have a computed field "A" and define it as "A = B × C" and we also know "C = D + E", we would only create one computed field "A" in the application where the equation would be "B × (D + E)".

While this approach can be verbose, it is sometimes the simplest.

Troubleshooting: Computed fields validation

Computed fields validation is complex since they are only valid in relation to the IBM OpenPages with Watson reporting framework, which may change in response to a change in the OpenPages with Watson object model.

Therefore, we provide several forms of validation.

When creating or editing a computed field, it is validated against the primary namespace as well as all alternate namespaces. If any of the validation checks fail, then the OpenPages with Watson application will not allow you to save the computed field until corrected. The OpenPages with Watson application maintains strict validation checks in this area because a slight error here can have an extensive ripple effect that is hard to identify and correct.

Also, due to the complexity of the computation engine there are certain cases where two computed fields will be valid by themselves but invalid together. A common example is where two computed fields reference different Object ID columns. In order for the computations to be grouped correctly they must all have the same Object ID column value. Therefore, we provide validation functionality across both an entire Field Group definition as well as an Object Type definition.

Troubleshooting: Computed field equation length limitation

Currently there is a limitation on the size of the computation attribute value that can be stored by the application.

The main attribute of concern is Equation where a complex equation could be very lengthy. There is a 20,000 byte limit on the size of the entered text. Note that IBM OpenPages with Watson supports multibyte characters and so this may not be the equivalent of 20,000 characters if you are using a multibyte language.

Troubleshooting: Computed fields with cross products

A cross product normally occurs when a table of data is joined with itself resulting in redundant data.

In the case of computed fields as they relate to Cognos we encounter a slightly more complex version.

For example, in the out-of-the-box ORM schema we have computed fields on the Loss Event object type that aggregate associated Loss Impacts and Loss Recoveries. In effect we are joining the Loss Event data with itself because we have two associations (joins) from the same object type and this causes a cross product.

If you have the following associations between Loss Event and Loss Impact:

- LE - LI1
- LE - LI2
- LE - LI3

And the following associations between Loss Event and Loss Recovery:

- LE - LR1
- LE - LR2

When a query is written to access all three object types the following data is returned:

- LE, LI1, LR1
- LE, LI2, LR1
- LE, LI3, LR1
- LE, LI1, LR2
- LE, LI2, LR2

- LE, LI3, LR2

In the case where we are aggregating values on the Loss Impact we end up with twice the desired value and on the Loss Recovery three times the value. One way to work around this is as follows:

Instead of:

```
total (Loss Impacts for Loss Events)
```

Use:

```
average (Loss Impacts for Loss Events) * count (distinct Loss Impacts for  
Loss Events)
```

Mathematically, we can say that $average \times distinct\_count = total/count \times distinct\_count = total \times distinct\_count/count$.

So if we are trying to total the Loss Impacts for a Loss Event in the previous example we would be performing a total on the cross product result and then multiplying by 1/2 to factor out the cross product. If we are trying to total the Loss Recoveries for a Loss Event in the previous example we would be performing a total on the cross product result and then multiplying by 1/3 to factor out the cross product.

Troubleshooting: Optimizing report request performance

With the addition of computed fields there is a large increase in the number of report requests and so it is important to make sure Cognos is set up correctly.

One common pitfall is the number of processes configured for the ReportService. This can be configured as follows.

Procedure

1. From a browser, log on to the IBM Cognos Analytics as a user with administrative privileges, for example, OpenPagesAdministrator.

By default, the URL is:

`http://<hostname>/ibmcognos/bi` (if you are using port 80 for Cognos)

Where <hostname> is the name of the Cognos server.

2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Status** tab, click the **System** link.
4. In the **Scorecard** pane, do the following:

a) Under **All servers**, click the name of the reporting server you want to tune.

b) Under the **reporting server**, click the name of the dispatcher. For example,
`http://<server_name>:9300/p2pd`

The dispatcher has the following icon  preceding its URI.

c) In the list of services for the dispatcher, click **ReportService**.

5. In the **Metrics - ReportService** pane, do the following:

a) Expand **Process**.

b) View and optionally edit the settings for the **Number of processes high watermark** and **Number of processes low watermark** performance metrics. These metrics monitor the maximum and minimum number of active user sessions since the last reset.

c) Expand **Queue**.

d) View and optionally edit the setting for the **Latency** performance metric. This metric specifies the average amount of wait time requests spend in the queue.

- e) Expand **Request**.
 - f) View and optionally edit the settings for the **Seconds per successful request** and **Successful requests per minute** performance metrics. These metrics specify the average number of seconds it takes to process a successful request and the average number of successful requests that can be processed in a minute.
6. In the **Settings - ReportService** pane, do the following:

Note: For information on performance metrics and additional settings that are not listed here, see the Cognos Analytics online Help.

- a) Expand **Tuning**.
- b) Change the value of the **Maximum number of processes for the report service during peak period** and **Maximum number of processes for the report service during non-peak period** settings. These settings specify the maximum number of child report service processes that can be started during peak demand and "off-peak" hours.

As a starting point, you should configure the value of these settings to be twice the number of CPUs on the Cognos server. For example, if your environment is always at peak and Cognos is running on a quad-CPU box, then you would set the maximum number of processes to 8 for each setting.

If slow computed fields performance is observed, you can visit the administration page again to observe the number of available processes as well as the latency. Note that these values are only meaningful on a system under load. If all the processes are consistently busy and there is a large latency to service a request, consider changing the number of processes.

Troubleshooting: Computed field query direction performance

While in Cognos it is possible to query up the relationship tree (that is, compute values based on ancestors), but it is strongly discouraged.

When exploring all the computation possibilities there is one large distinction in what can and should be done. The automatic framework generation is set up in such a way as to create joins that are conducive to better performance querying down the relationship tree. A query up the tree will result in bad computed field performance as well as place a large strain on the Database that can result in the entire application slowing down.

Adding enumerated string values (Standard UI)

You can add new values to an existing list of enumerated string values at any time. The modifications you make to values in a list are globally applied to all instances wherever that field group is in use.

For example, you created an object field called "Rating" that was an Enumerated String data type. When the field was initially created, it was given the following values: High, Medium, and Low. Because of changing business needs, you want to add a new value of "Unknown" to the list. You could add this new value at any time and have it immediately displayed to users as a selection in the list of values.

When you add a new string value to an existing list of values:

- The value is immediately displayed to users for selection in the list of values
- The new value is added to the end of the value list

Procedure

1. Click **Administration > Field Groups**.
2. On the **Field Groups** table, click the name of the field group in the list that contains the field you want to modify.
3. On the **Field Definitions** table of the selected field group details page, click the name of the field that contains the enumerated string that you want to modify.

4. On the **Enumerated String Values** table of the field definition details page:
 - a) Click **Add**.
 - b) In the **Name** box, type a value for the new string.
 - c) Click **Create**.
5. To change the order number of the string values, see [“Changing the order of enumerated string values \(Standard UI\)”](#) on page 233.

Defining a default value for an enumerated string value (Standard UI)

You can define a default value for an enumerated string value. When you define a default value, it is automatically applied to new objects that you create, but it is not applied to existing objects.

If you define a multi-select enumerated field value as the default value, and the field is hidden, users can see the hidden field value in the Add New wizard because the default attribute overrides the hidden attribute.

Procedure

1. Click **Administration > Field Groups**.
2. On the **Field Groups** table, click the name of the field group in the list that contains the field you want to modify.
3. On the **Field Definitions** table of the selected field group details page, click the name of the field that contains the enumerated string that you want to modify.
4. On the **Enumerated String Values** table of the field definition details page, click **Edit**.
5. Update the **Default Value**.
6. Click **Save**

Changing the order of enumerated string values (Standard UI)

For object fields with an Enumerated String data type, you can modify the order in which string values are displayed to users.

This topic applies only to the Standard UI.

When you change the order number of a string value, all the string values following the changed order number are dynamically updated by the system.

For example, the display order of string values in a list is: High 1, Medium 2, Low 3, Unknown 4. If you want Unknown to be displayed first in the list, you would change the order number of Unknown from 4 to 1. The system will automatically reorder the other string values. The new order of the string values in the list displays as: Unknown 1, High 2, Medium 3, Low 4.

Procedure

1. Click **Administration > Field Groups**.
2. On the **Field Groups** table, click the name of the field group in the list that contains the field you want to modify.
3. On the **Field Definitions** table of the selected field group details page, click the name of the field that contains the enumerated string that you want to modify.
4. On the **Enumerated String Values** table of the field definition details page:
 - a) Find the rows containing the string value whose list order you want to change.
 - b) In the **Order** boxes, type a new order number for the values.
 - c) Click **Update Order**.

Hiding enumerated string values (Standard UI)

You can hide obsolete or unwanted string values from a list of enumerated string values.

This topic applies only to the Standard UI.

When you hide a string value from a list:

- For new instances of an object, the value or values are immediately hidden from selection by users on the list of values.
- For existing instances of an object, if the value or values were previously selected by users (that is, before the value was hidden), the value or values are still displayed in the list and are available during editing for selection by users.
- The "Hidden" column on the **Enumerated String Values** table changes from "false" to "true".

If you define a multi-select enumerated field value as the default value, and the field is hidden, users can see the hidden field value in the Add New wizard because the default attribute overrides the hidden attribute.

Procedure

1. Click **Administration > Field Groups**.
2. On the **Field Groups** table, click the name of the field group in the list that contains the field you want to modify.
3. On the **Field Definitions** table of the selected field group details page, click the name of the field that contains the enumerated string that you want to modify.
4. On the **Enumerated String Values** table of the field definition details page:
 - a) Select the box next to the value or values you want to hide from the list. The "Hidden" column for the value will be set to "false".
 - b) Click **Hide/Unhide**. The "Hidden" column for the value changes to "true".

Note: The **Hide/Unhide** icon toggles between **Hide** and **Unhide** depending on the current setting.

Unhiding enumerated string values (Standard UI)

If an enumerated string value was previously hidden from visibility by users, you can "unhide" the hidden value and make it again visible to users in the list.

When you unhide a string value from a list, the following occurs:

- The value is immediately displayed for selection by users on the list of values.
- The "Hidden" column on the **Enumerated String Values** table changes from "true" to "false".

Procedure

1. Click **Administration > Field Groups**.
2. On the **Field Groups** table, click the name of the field group in the list that contains the field you want to modify.
3. On the **Field Definitions** table of the selected field group details page, click the name of the field that contains the enumerated string that you want to modify.
4. On the **Enumerated String Values** table of the field definition details page:
 - a) Select the box next to the hidden value or values you want to display from the list. The "Hidden" column for the value will be set to "true".
 - b) Click **Hide/Unhide**. The "Hidden" column for the value changes to "false".

Note: The **Hide/Unhide** icon toggles between **Hide** and **Unhide** depending on the current setting.

Deleting enumerated string values (Standard UI)

You can only delete an enumerated string value from a field definition if the field group containing the field is not in use.

A deleted string value is permanently removed from the list and cannot be retrieved. If the field group is in use, **Delete** remains disabled and you can only hide any obsolete or unwanted string values from view. For details see, [“Hiding enumerated string values \(Standard UI\)”](#) on page 234.

Procedure

1. Click **Administration > Field Groups**.
2. On the **Field Groups** table, click the name of the field group in the list that contains the field you want to modify.
3. On the **Field Definitions** table of the selected field group details page, click the name of the field that contains the enumerated string that you want to modify.
4. On the **Enumerated String Values** table of the field definition details page:
 - a) Select the box next to the name of the value you want to remove - **Delete** becomes enabled.
Note: If **Delete** remains disabled, the field group to which this field definition belongs is in use and you cannot delete the value.
 - b) Click **Delete**.

Adding a currency field to a field group (Standard UI)

You can add a currency field to a field group.

Procedure

1. Click **Administration > Field Groups**.
2. In the **Field Groups** table, click the name of the field group to which you want to add a currency field. The page containing information for that field group appears.
3. In the **Field Definitions** table, click **Add**. The page containing the information to add the field definition appears.
4. On the add page:
 - a) In the **Name** box, type a name for the new currency field.
 - b) Select **Currency** from the **Data Type** drop-down list.
Important: Do not change or translate currency codes.
 - c) Check **Required** if the field is to be a required field.
Note: The Currency data type does not support computed fields. See [“Defining a computed field”](#) on page 227 for information on computed fields.
 - d) Check **Include Conversion** if the field is to include currency conversion.
 - e) Click the >> icon and type the minimum and maximum allowable currency values to be allowed in the field in the **Minimum Value** and **Maximum Value** boxes.
 - f) Click **Create**. The system creates the new currency field.

Note:

- If a user enters a value that is either below or above the specified value range, an error message displays.
- You cannot use non-numeric characters when entering currency values. For example, either 125000 or 125,000 is legal, but not \$125000.
- This format is set per User Locale.

- Object fields with this data type cannot be included in the profile of predefined objects or custom forms that use the supplied JSP file for rendering.

Editing currency field information (Standard UI)

You can edit currency field information.

Procedure

1. Click **Administration > Field Groups**.
2. In the **Field Groups** pane, click the name of the field group that contains the currency field to edit.
3. In the **Field Definitions** pane, click the name of the currency field to edit.
 - a) Click **Edit**.
4. Edit the information.
5. Click **Save**.

Viewing and editing a currency display type (Standard UI)

You can view and edit currency display type information for object types that contain a currency field.

Procedure

1. Click **Administration > Profiles**.
2. Click the name of the profile that contains both the object type and currency field you want to view or edit.
3. Click the object type.
For example, to view or edit the currency display type for the **Inherent Severity** object field, select the **SOXRisk** object type.
4. Click the desired object field. The **Display Type** column of the selected field should be 'Currency'.
On the detail page of the selected object field, the currency display information appears.
5. To edit the currency display type, complete the following actions:
 - a) Click **Edit**.
 - b) Set the read only value to True or False.
 - c) To set the field as required, select **Required**.
 - d) Click **Save**.

Editing currency field values in individual accounts (Standard UI)

If you have IBM OpenPages Financial Controls Management installed, you can edit currency field values for individual accounts.

Procedure

1. Log on to the IBM OpenPages with Watson application.
2. From the menu bar, select **Financial** and click **Accounts**.
3. From the list, click the name of the account you want to open its details page.
4. Under **Account Details**, click the **Fields** link.
5. Select the **Actions** menu and choose **Edit this Account**.
6. In the **Annualized Value** field, change the Currency, Exchange Rate, or USD values as desired.
7. When finished, click **Save**.

Modifying currency exchange rates (Standard UI)

You can add, edit, enable, and disable currency exchange rates.

About this task

For more information, see [“Modifying currency exchange rates” on page 213](#).

Uploading a CSV file (Standard UI)

You can upload currency rates from a CSV file.

Before you begin

Create the CSV file. For more information, see [“Formatting a CSV file” on page 214](#).

Procedure

1. Click **Administration > Currencies**.
2. On the Currencies page, click **Upload**.
3. Type the CSV file name into the **Exchange Rates File Name** box or select the appropriate file by clicking **Browse**.
4. Click **Upload**. The new currency exchange rate appears in the Currencies table on the Currencies page.

Editing exchange rates for an existing currency code (Standard UI)

One of the ways to modify an exchange rate for an existing currency code is to use the Standard UI.

Procedure

1. Click **Administration > Currencies**.
2. On the **Currencies** page, click **Edit**.
3. On the **Edit Exchange Rate** page, edit the currency exchange rates as needed.
An exchange rate is the amount of a currency per unit of the system base currency.
4. Click **Save**. The edited currency exchange rates appear on the Currencies page.

Enabling currency exchange rates (Standard UI)

You can enable disabled currency rates, making them available to the appropriate processes.

Procedure

1. Click **Administration > Currencies**.
2. On the **Currencies** page, click **Enable**.
3. On the **Enable Currencies** page, check all the currencies you want to enable.
4. Optional: Change the exchange rate for any listed currencies.
5. Click **Save**. The enabled currencies appear on the Currencies table.

Disabling currency exchange rates (Standard UI)

You can disable enabled currencies. When you disable a currency it is no longer available to the system. However, it is not deleted. You can enable it at any time.

Note: You cannot enable or disable the base currency, which is set during installation.

Procedure

1. Click **Administration** > **Currencies**.
2. On the **Currencies** page, click the check box next to the currencies you want to disable. (You can re-enable these currencies at any time.)
3. Click **Disable**.

Reporting fragment fields

Reporting fragment fields are always read-only fields that typically display a component (such as a chart or table) from a larger Cognos report.

Reporting fragment fields are configured in a number of ways:

- Associate with an object type
- Add to various object view pages
- Configure as dependent fields
- Modify their display type

By default, reporting fragment fields have a display type of Automatic for Detail and Activity View pages and the report component is embedded directly on the page. If the display type is changed to On Demand, the report component is displayed in a pop-up window. Pop-up windows can be autosized through settings in the application or manually overridden when the reporting fragment field is defined.

Limitations

Reporting fragment fields have the following limitations:

- You cannot use elements from JSP reports in reporting fragment fields; only components from Cognos reports are supported.
- Page breaks in reporting fragment fields are not supported.
- Tooltips in reporting fragment fields are not supported.
- A report that has required prompts other than Object ID and Reporting Period ID cannot be used as a reporting fragment field.

Note: See the *IBM OpenPages with Watson Report Author's Guide* for information about designing reports that can be used in reporting fragment fields.

Tasks for configuring reporting fragment fields

Use the following configuration tasks to set up new reporting fragment fields.

Table 97. Tasks for configuring reporting fragment fields	
Task Description	Related Topic
Identify the Cognos report and report component and the field group you want to use.	“Planning considerations for reporting fragment fields” on page 239
From Cognos, obtain the parameter information for the reporting fragment field.	“Fields requiring parameter information” on page 239
In the IBM OpenPages with Watson application, define the reporting fragment field.	“Defining a reporting fragment field” on page 240

Table 97. Tasks for configuring reporting fragment fields (continued)	
Task Description	Related Topic
Add the field group to an object type if it is not already included.	“Including field groups for an object type (Standard UI)” on page 255
Select a profile and add the reporting fragment field to an object type in that profile.	“Including fields in an object type” on page 306
Select an object view in that profile and add the reporting fragment field to that view page.	“Configure views for objects” on page 322
Optionally, change the display type and display characteristics.	“Configuring the display type for reporting fragment fields (Standard UI)” on page 348

Planning considerations for reporting fragment fields

Before you add a reporting fragment field, you need to identify the report with the component you want, and which object types, profiles, and object views will be associated with the reporting fragment field.

Planning your changes ahead of time helps to minimize the necessary work and prevents duplication of effort.

The following list will help you identify some of the questions you need to consider before you create a new reporting fragment field:

- Report component — What report component data does the user need to see to accomplish their task? Which Cognos report contains the component?
- Field group — Will new reporting fragment fields reside in new or existing field groups?
- Object type — Which object type will use the reporting fragment field or fields?
- Views — Which view pages in a profile will use the reporting fragment fields (such as Filtered List View, Detail View, Activity View, My Work tab)?
- Display — How many reporting fragment fields will be included in a Detail or Activity View page? Will a reporting fragment field be embedded (Automatic) on the page or displayed as a pop-up window (On Demand)?

Fields requiring parameter information

The process of creating a new reporting fragment field for use in the IBM OpenPages with Watson application involves copying parameter information from Cognos and either pasting or entering it into fields on the Reporting Fragment data type field definition page in the IBM OpenPages with Watson application.

Note: You must have administrative privileges set on your account so you can access:

- The IBM Cognos Analytics and IBM Cognos Analytics - Reporting for obtaining parameter information
- The IBM OpenPages with Watson application for defining the new reporting fragment field

Table 98 on page 240 lists the various fields on the Reporting Fragment data type field definition page that require specific parameter information.

Table 98. Required parameter information		
Fields	Field description	Where to find the parameter information
Report Path	Required. The file path of the selected Cognos report that contains the component you want to use. “Defining the report path” on page 241	Cognos Analytics, Team content folder
Fragment Name	Required. The unique name of the particular report component (such as a ‘Pie Chart’, ‘List’, ‘Combination Chart’, and so forth). “Defining the reporting fragment name” on page 241	IBM Cognos Analytics - Reporting, Report Page
Object ID Prompt	Required only if the report prompts users to select a resource (such as ‘Entity’, ‘Process’, and so forth) before running the report. Otherwise, leave this field blank. “Defining the object ID prompt” on page 242	IBM Cognos Analytics - Reporting, Prompt Page
Reporting Period ID Prompt	Required only if the report prompts users to select a reporting period before running the report. Otherwise, leave this field blank. “Defining the reporting period ID prompt” on page 243	IBM Cognos Analytics - Reporting, Prompt Page

Defining a reporting fragment field

When defining a reporting fragment field, some tasks are required and some tasks are optional.

For purposes of illustration, the following tasks use examples from a sample Assessment Status report to configure a reporting fragment field that will display the chart component of this report as an embedded report on a Risk Assessment Detail View page.

Table 99. Tasks to define a reporting fragment field	
Task	Required or optional
“Setting up a field group for a new reporting fragment field” on page 241	Required.
“Defining the report path” on page 241	Required.
“Defining the reporting fragment name” on page 241	Required.
“Defining the object ID prompt” on page 242	Required only if a report prompts users to select a resource (such as ‘Entity’, ‘Process’, and so forth) before running the report. Otherwise, skip this task and leave the field blank.
“Defining the reporting period ID prompt” on page 243	Required only if a report prompts users to select a reporting period before running the report. Otherwise, skip this task and leave the field blank.
“Defining the reporting fragment size” on page 243	Optional. Use if you want to manually control the height and width of the pop-up window for a fragment field.

Setting up a field group for a new reporting fragment field

You can use either an existing field group or create a new field group for the new reporting fragment field.

Before you begin

Complete the following steps to set up a field group for a new reporting fragment field:

Procedure

1. Access the **Field Groups** page. See [“Defining field groups” on page 206](#).
2. To include the reporting fragment field in an existing field group, click the name of the field group.
3. To include the reporting fragment field in a new field group, see [“Defining field groups” on page 206](#).
4. On the detail page of the field group, navigate to the **Field Definitions** pane and click **Add**.
5. On the field definitions detail page, type the name of the object field.
6. Click **Reporting Fragment** from the **Data Type** field.
7. Click the double arrow  next to the data type selector to display additional parameters.

Note: Keep the browser window open because you will return to it.

Defining the report path

To define the report path, gather information from both the IBM Cognos Analytics and IBM OpenPages with Watson to obtain path information for the report.

Procedure

1. Configure your environment to use the Cognos 10 home page, IBM Cognos Connection.
See [How to display the version 10 Cognos Connection home page in Cognos Analytics 11](#).
2. Open IBM Cognos Connection.
3. Click the **Team content** folder and navigate through the folder hierarchy to the report location.

For example,

Team content > OpenPages Solutions V6 > Risk Assessment Reports >
Risk Assessment Status

4. In the **Actions** column for the report, click the **Set Properties** icon .
5. On the **Set Properties** page of the report, select **General**.
6. Click the **View the search path, ID and URL** link.
7. Copy the text in the **Search path** field.

The following example is a sample search path text for the Risk Assessment Status report.

```
/content/folder[@name='OPENPAGES_PLATFORM']/folder[@name='Risk  
Assessment Reports']/report[@name='Risk Assessment Status']
```

8. In OpenPages with Watson, go to the **Reporting Fragment field definitions detail** page and paste the search path text into the **Report Path** field.
9. Click **Launch > IBM Cognos Administration**.
10. Remove the portal.disable advanced setting that you added in step 1.

Defining the reporting fragment name

To define the reporting fragment name, the steps in this task require going back and forth between the IBM Cognos Analytics and the IBM OpenPages with Watson application user interface to obtain the name of the report component within the selected report.

Before you begin

Complete the following procedure to define the reporting fragment name:

Procedure

1. In IBM Cognos Analytics - Reporting, open the report containing the component you want:
 - a) On the Team Content tab, navigate through the folder hierarchy to where the report you want is saved.

For example, Team Content > OpenPages Solutions V6 > Risk Assessment Reports > Risk Assessment Status
 - b) Under the Actions column for the report you want, click **Edit report**.
2. In edit mode, select the component you want to use for the Reporting Fragment field (such as a List, a Chart, a Crosstab, and so forth.)
3. Verify that the entire component is selected:
 - a) Click **Show Properties** in the application bar.
 - b) In the **Properties** pane, look at the title bar. It should display the name of the selected component, such as Pie Chart, List, Combination Chart, and so forth.
 - c) If the Properties title bar displays the name of a subcomponent (for example List Column Body or List Column Title), then click the Properties up arrow icon on the Properties title bar and select the entire component (for example, List).
4. In the Properties pane, under the **Miscellaneous** heading, copy the value in the **Name** property.

For example, the Name property value for the Combination Chart component of the sample Risk Assessment Status report is Combination Chart1.
5. In OpenPages with Watson, on the Reporting Fragment field definitions detail page, paste or type the value into the **Fragment Name** box.

For example, for the sample Risk Assessment Status report, you would paste or type Combination Chart1.

Note: If the report prompts for an object or reporting period ID, keep the report open in IBM Cognos Analytics - Reporting.

Defining the object ID prompt

To define the Object ID Prompt, the steps in this task require going back and forth between the IBM Cognos Analytics and the IBM OpenPages with Watson application user interface.

Note: This task is required only if a report prompts users to select a resource (such as Entity, Process, and so forth) before running the report. Otherwise, skip this task and leave the field blank.

Procedure

1. In IBM Cognos Analytics - Reporting, open the report:
 - a) On the Team Content tab, navigate through the folder hierarchy to where the report you want is saved.

For example, Team Content > OpenPages Solutions V6 > Risk Assessment Reports > Risk Assessment Status
 - b) Under the Actions column for the report you want, click **Edit report**.
2. For the selected report:
 - a) Click **Pages**.
 - b) Navigate to the prompt page of your report.

3. On the prompt page:

- a) Click the prompt for the object identifier (such as Entity, Process, and so forth).
- b) Click **Show Properties** in the application bar.
- c) Under the **General** heading, click the **Parameter** property icon and copy the value in the box (for example, Entity).

For example, the sample Risk Assessment Status report prompts users to select a Business Entity before running the report. On the sample Risk Assessment Status report PromptPage, you would select the Value Prompt object for Business Entity. The value in the Properties - Value Prompt for the Parameter field is Entity.

4. In OpenPages with Watson, on the Reporting Fragment field definitions detail page, paste or type the value into the **Object ID Prompt** box.

For example, for the sample Risk Assessment Status report, you would paste or type Entity in the Object ID Prompt box.

Defining the reporting period ID prompt

To define the Reporting Period ID Prompt, the steps in this task require going back and forth between the IBM Cognos Analytics and the IBM OpenPages with Watson application user interface.

Note: This task is required **only** if a report prompts users to select a reporting period before running the report. Otherwise, skip this task and leave the field blank.

Procedure

1. In IBM Cognos Analytics - Reporting, open the report:

- a) On the Team Content tab, navigate through the folder hierarchy to where the report you want is saved.

For example, Team Content > OpenPages Solutions V6 > Risk Assessment Reports > Risk Assessment Status

- b) Under the Actions column for the report you want, click **Edit report**.

2. For the selected report:

- a) Click **Pages**.
- b) Navigate to the prompt page of your report.

3. On the prompt page:

- a) Click the prompt for the reporting period identifier.
- b) In the **Properties** pane, scroll to the **General** heading.
- c) Under the **General** heading, click the **Parameter** property icon and copy the value in the box.

4. In OpenPages with Watson, on the Reporting Fragment field definitions detail page, paste or type the value into the **Reporting Period ID Prompt** box.

Defining the reporting fragment size

When defining the reporting fragment size, if you leave the pixel values for height and width blank (this is the default), the pop-up window is sized automatically.

This task is optional. Use if you want to manually control the height and width of the pop-up window for a reporting fragment field.

Procedure

1. In IBM OpenPages with Watson, on the **Reporting Fragment field definitions detail** page:

- a) In the **Height** box, type a numeric value for the pixel height of the reporting fragment.
 - b) In the **Width** box, type a numeric value for the pixel width of the reporting fragment.
2. Click **Save**.

Using object fields to launch JavaServer Pages and external URLs

You can customize the OpenPages application to launch JavaServer Pages (JSPs) or external URLs from object fields. You can pass arguments to the JSP or external URL in a URL configuration string that is defined on the object field.

The launchers use simple string fields with a URL display type to show a labeled hyperlink in the application. The URL parameters for the hyperlink can contain system-generated elements, such as the ID of the target object and the current reporting period. The availability of the hyperlink can be controlled by a set of conditions. For example, the link is active when the current user is the Process Owner and they select the current Reporting Period.

The attributes for the launchers are specified by using a URL configuration string that is defined as the default value for the object field, called a URL launcher field in this context. The application processes the configuration string when an object view that contains the URL launcher field is rendered. You can add launchers to Detail, Activity, Filtered List Views, and Grid Views. You define the hyperlink's label using application text. You can make the label meaningful for your users. For external URLs, you can make the label a short name that users know rather than a long URL.

To set up a URL launcher field:

1. Define the URL configuration string. Learn about the attributes in the string and study the examples. For information, see [“Attributes in the URL configuration string” on page 244](#) and [“URL configuration string examples” on page 246](#).
2. Define the URL launcher field and add the URL configuration string to it. For information, see [“Adding a URL launcher field ” on page 248](#) .
3. Define the label for the URL launcher field in application text. For information, see [“Configuring application text” on page 247](#).
4. Add the URL launcher field to views in the Standard UI. For information, see [“Adding a URL launcher field to views” on page 248](#).
5. Add the URL launcher field to views in the Task Focused UI. For information, see [“Displaying a URL launcher field as a button or link” on page 410](#).

Attributes in the URL configuration string

The URL configuration string is in JSON format.

It uses the following attributes:

- labelKey
- path
- parameters
- conditions
- popUp

labelKey attribute

Identifies the application text key for the localized URL text. If it is omitted, the label defaults to **Go**.

path attribute

Specifies the relative path to the target JSP, report, or application object view. If the target is a JSP, then it must be in a folder that is under the sosa application deployment folder. The path attribute is required.

The application root is automatically prepended to the specified path by the application. The application root is determined from the **application.url.path** property in the `Server<#>-sosa.properties` configuration file.

The path value must contain the leading slash. For example, "path" : `"/custom/mycustom.jsp"`,

modes attribute

Controls whether the URL launcher field is available in edit or view mode.

In order for a URL launcher field to appear in an Activity View Child Hierarchy pane, the "Edit" mode must be included.

parameters attribute

Contains the list of request parameters that are assembled to create the query string of the URL. The parameters are specified as a list of key-value pairs. In most instances, the key names can be anything that you define.

System-populated keys and values are indicated by a \$ in the name. They consist of:

- the ID of the current object, indicated by a parameter value setting of "\$objectId"
- the ID of the current reporting period selection, indicated by a parameter value setting of "\$reportingPeriodId"

Any subset of these parameters can be specified.

Hardcoded parameter values can also be included. For example, where the target JSP or report is reused in different contexts and requires additional information to identify the context for this specific URL launcher field.

The URL parameter values are URL encoded, while the keys are not.

conditions attribute

Defines conditions that must be met in order for the URL to be active.

The conditions can include the following:

- Whether the Reporting Period selected is the current period.
- Whether the target object is locked.
- Whether the value of a specific field matches a value.
- Whether the value of a specific field matches the name of the current user.
- Whether the current user is a member of the group name set in a specific field.

Any subset of the available conditions can be included in the URL configuration string. These conditions are evaluated in the order in which they appear in the string. Each condition can optionally include a labelKey that contains an application text string that is displayed when a condition is not met, for example, "Available only for the Process Owner." If the labelKey is omitted, the key for the field is applied.

Multiple conditions of the same type can be used, except for the objectState and reportingPeriod conditions. You can use only one objectState and one reportingPeriod.

Most errors in the configuration of a condition cause a positive failure in the condition and evaluate to true. The errors are logged. Thorough testing of both positive and negative cases is encouraged to ensure the expected behavior.

reportingPeriod condition

The reportingPeriod condition is met when:

- The value of "isCurrent" is true and the user is in the current Reporting Period.

- The value of "isCurrent" is false and the user is in any previous Reporting Period.

objectState condition

The objectState condition is met when:

- The value of "isUnlocked" is true and the current object is not locked.
- The value of "isUnlocked" is false and the current object is locked.

fieldValue condition

The fieldValue condition evaluates the value of the field against the value that is specified by the value attribute by using the specified operator. The target field is identified by using the FieldGroup.FieldName convention. The supported operators are "equal" and "notEqual". If the operator is invalid or omitted, the evaluation defaults to "equal".

The Simple String, Boolean, and Enumeration field types are supported. Ensure that you specify the system name and not the localized label for the enumeration values.

The fieldValue condition supports checking the current user—by specifying "\$currentUser"—against the value of the target field.

The fieldValue condition does not support system fields ("Created by" and "Modified by") or multi actor fields.

popUp attribute

Controls the behavior of the new window. The "windowAttributes" string determines the characteristics, such as size and scroll bars, of the new window that is created when the user clicks the hyperlink. The popUp attribute is optional.

URL configuration string examples

The following examples illustrate how to define URL configuration strings.

Launching a custom JSP with a popup

The following example launches a custom JSP.

```
$ {
  "labelKey" : "custom.url.labelForMyCustomUrl",
  "path" : "/custom/mycustom.jsp",
  "modes" : ["edit", "view"],
  "parameters" :
  {
    "objId" : "$objectId",
    "repId" : "$reportingPeriodId",
    "isRisk" : "true",
    "includeVersions" : "false"
  },
  "conditions" :
  {
    "reportingPeriod" :
    {
      "isCurrent" : true/false, // no quotes for boolean values
      "labelKey" : "custom.url.label.invalid.ReportingPeriod"
    },
    "objectState" :
    {
      "isUnlocked" : true/false, // note the UN-locked designation
      "labelKey" : "custom.url.label.object.locked"
    },
    "fieldValue" :
    {
      "field" : <"FieldGroup.FieldName">,
      "value" : "$currentUser",
      "operator" : "equal", // supported operators include "equal" and "notEqual"
      "labelKey" : "custom.url.label.invalid.user"
    }
  }
}
```



```

    }
    "fieldValue" :
    {
        "field" : <"FieldGroup.FieldName">,
        "value" : true,
        "labelKey" : "custom.url.label.invalid.value"
    }
    "fieldValue" :
    {
        "field" : <"FieldGroup.FieldName">,
        "value" : "Undifferentiated",
        "operator" : "notEqual",
        "labelKey" : "custom.url.label.invalid.value"
    }
    },
    "popUp" :
    {
        "windowAttributes" : "height=600,width=800,menubar=no,status=yes,toolbar=no,
scrollbars=yes,resizable=yes"
    }
}

```

Launching a Cognos report

The following example launches a Cognos report from a Command Center redirect with a security condition:

```

${
  "labelKey": "report.name.security.domain.role.assignments",
  "path": "/report.tree.post.do",
  "modes": ["view"],
  "parameters": {
    "reportPath": "/_cw_channels/Reporting/SOX/OpenPages V6/Audit Reports/Security/Security
Domain Role Assignments.pagespec",
    "label": "Current Reporting Period",
    "submitAction": "preview",
    "actionContext": "preview",
    "entity_id": "$objectId"
  },
  "conditions": {
    "fieldValue": {
      "field": "OPSS-BusEnt.Executive Owner",
      "value": "$currentUser",
      "operator": "equal",
      "labelKey": "custom.url.invalid.user"
    }
  }
}
}
}

```

Launching a custom JSP

The following example launches a custom JSP.

```

$ {
  "labelKey" : "url.custom.jsp",
  "path" : "/custom/custom.jsp",
  "modes" : [ "view", "edit" ],
  "parameters" :
  {
    "Risk Category" : "Damage to Physical Assets",
    "Risk Sub-category" : "Willful Damage"
  }
}

```

Configuring application text

You can add translated labels for the keys that you specify in the URL configuration string.

Procedure

1. Under **Administration**, click **Application Text**.

2. In the Custom line, click **Add New**.
3. Enter the key value in **Name**.
4. Enter useful information, for example, the URL field that uses the key, in **Description**.
5. Enter the label text in **Default Label**.
6. Click **Create**.
7. Expand the new key, and add the translated text.
8. Repeat these steps for each key in the URL configuration string.

Adding a URL launcher field

The URL launcher field is defined with the URL configuration string as the default value.

Before you begin

Define the URL configuration string before you create the URL launcher field.

Procedure

1. Under **Administration**, click **Field Groups**.
2. Click **Add**.
3. Enter a **Name** and **Description** for the field, and click **Create**.
4. In the list of field groups, click the field group that you added.
5. In the Field Definitions table, click **Add**.
6. Enter the information for the field:
 - a) Enter a system name for the field.
 - b) In the **Data Type** box, select **Simple String**, and click the arrow to add it.
 - c) Set the **Default Value** to the URL configuration string.
 - d) Clear the **Required** and **Computed** boxes.
 - e) Click **Create**.

Adding a URL launcher field to views

Add the URL launcher field to the object type and then to the views.

Procedure

1. Under **Administration**, click **Object Types**.
2. Select the object type that you want to add the URL launcher field to.
3. In the **Included Field Groups** section, click **Include**, select the field you created in [“Adding a URL launcher field”](#) on page 248, and click **Add**.
4. Under **Administration**, click **Profiles**.
5. Select a profile you want to update.
6. Click the object type that contains the new field.
7. Click **Include**, select the new field, and click **Include**.
8. Click the newly added field, and in the **Object Field Information** pane, click **Edit**.
9. Change the **Display Type** to URL, and click **Save**.
10. Go back to the profile detail page and click the name of a view that you want to add the field to.
11. In the **Included Field Groups** section, click **Include**, select the new field, and click **Include**.
12. Select **Read-Only** for the field, and click **Save**.

Chapter 10. Object types

An object type contains metadata about a category of object, such as a Risk or Process object, or a custom form.

From an Object Type page, you can view and access the following information:

- Property information about the object type (such as name, labels, description)
- Field groups, with their field definitions, that are included in this object type
- Allowed parent and child relationships (associations) to other object types
- Filters that are used to narrow the scope of data for this object type
- Dependent fields and pick lists that have been defined for this object type
- Fields for this object type that have been excluded from one or more subsystems
- Facts and dimensions that are configured for this object type that can be generated by the reporting framework

An object type is identified in the Standard UI by the **Object Type** icon . Each object type includes field groups and associations to other objects.

For custom forms, such as surveys, you must add an object type for each custom form that you create. For more information, see [“Tasks required to set up custom forms” on page 265](#).

Related information

- Viewing object types in object model diagrams, see [“Solution schema visualizations ” on page 250](#).
- Configuring groups, fields, field groups, and filters on object types by using the Task Focused UI, see [“Working with object types \(Task Focused UI\)” on page 253](#).
- Configuring groups and fields for an object type by using the Standard UI, see [Chapter 9, “Fields and field groups,” on page 199](#).
- Customizing text labels for object types, see [Chapter 17, “Localizing text,” on page 559](#).
- Configuring facts and dimensions in the reporting framework, see [“Facts and dimensions” on page 953](#).

Note: If the same management operation is being modified by another administrator, an error message is displayed requesting that you try again later.

Platform object types

The IBM OpenPages with Watson object model is configurable and can contain object types.

Because the object types and schema vary widely from customer to customer, [Table 100 on page 249](#) lists only the Platform object types that are installed, by default, on all systems.

Table 100. Platform object types		
Icon	Object Name	Singular Label
	SOXBusEntity	Business Entity
	SOXIssue	Issue
	SOXTask	Issue Action Item
	SOXDocument	File
	SOXExternalDocument	Link

Table 100. Platform object types (continued)		
Icon	Object Name	Singular Label
	SOXSignature	Signature
	SOXMilestone	Milestone
	ProjectActionItem	Milestone Action Item
---	SOXProject	Project

Note: The SOXProject object type is for system use only; it is the master parent object type for all top level Business Entities and Milestones.

Solution schema visualizations

OpenPages is delivered with system object models that you can view in the solution schema visualization editor. You can also use the editor to create your own solution schema visualizations.

OpenPages is delivered with the following system object models:

- One global object model
- An object model for each OpenPages solution

The solution schema visualization editor is a tool that you can use to view these object models as object model diagrams. In this context, the term *solution* refers to visualizations for object models, be they system object models or solution visualizations that you create.

Using the solution schema visualization editor

Use the solution schema visualization editor to view the OpenPages object models as object model diagrams and create new solution schema visualizations.

To open the solution schema visualization editor, access the Task Focused UI and click  > **System Configuration** > **Solutions**. Whether the menu item is displayed depends on your access permissions.

Solutions List

The Solutions List shows system object models and user-created solution schema visualizations. From the Solutions List, you can:

- Click a solution. The solution opens in the solution schema visualization editor.
- Click the Name column header to change the sort order of the list.
- Select the checkbox next to a single solution or multiple solutions to update numerous solutions. The bulk update options are:

- Delete

Clear the check boxes to hide the bulk update options.

System object models cannot be deleted.

- Click  to open a Quick View panel where you can view a list of object types in a solution. For user-created solution schema visualizations, you can also add and remove object types.
- Click **Add New** to create a new solution schema visualization. After you define the initial properties, the visualization editor opens. For more information, see [“Creating a solution schema visualization”](#) on page 252.

Solution schema visualization editor

Select a solution in the Solutions List and the solution schema visualization editor opens. It has two tabs:

- Map View
- Grid View

Map View

The Map View shows one solution. It has the following components:

- Canvas

The canvas shows the object model diagram, including directional arrows that indicate relationships.

- Click an object type on the canvas and information about the object type displays in the property panel.
- Move and rearrange the object types.

- Toolbar

Icons on the toolbar allow you to control the view on the canvas.

- Object Types list panel

The Object Types list panel shows all object types in the solution. It can be displayed or hidden.

- Click an object type in the Object Types panel and it is highlighted in the object model diagram.

- Click  to show an object type that is hidden. Use this icon to control the object types that are displayed on the canvas.

- Property panel

The property panel shows information about a selected object type. It can be accessed from the Map View or the Grid View.

- Expand the **Fields** folder to view a list of field groups that are assigned to the object type. Click a field group to view a list of fields that belong to it.

- Click  next to a field group to view a list of other object types that use the field group.
 - Click a field name to view it.

- Expand the **Relationship** folder to view a list of parent and child objects types that are associated to the object type.

- Expand the **Profiles** folder to view a list of profiles that are assigned to the object type.

- Expand the **Filters** folder to view a list of filters that are assigned to the object type.

- Expand the **Views** folder to view a list of Task Focused UI views that are assigned to the object type. Click a view to open it in a new tab.

- Expand the **Workflows** folder to view a list of workflows that are assigned to the object type. Click a workflow to open it in a new tab.

The Map View contains the following icons:

Table 101. Icons in the solution schema visualization editor	
Icon	Description
	Changes arrangement based on relationship.
	Resets the zoom.
	Expands (zooms in) the view.

Table 101. Icons in the solution schema visualization editor (continued)	
Icon	Description
	Shrinks (zoom out) the view.

Grid View

The Grid View shows a list of all object types that belong to a solution.

Click an object type, and it opens in the property panel (see description above).

Click **Show profiles** to display a matrix of object types and profiles that are assigned to them. Select and clear the check boxes to make bulk update changes to profile assignments. If you add a profile, all fields are added. Take care not to clear and re-select profiles because customizations to field assignments are lost and all fields are re-added.

Creating a solution schema visualization

Use the solution schema visualization editor to create new visualizations. For example, you can build visualizations for issue management or loss event management solution schemas.

About this task

A solution schema visualization provides access to object types and relationships.

Procedure

1. Click  > **System Configuration** > **Solutions**.
2. Click **Add New**.
3. Enter an internal **Name** for the solution. It cannot be changed later.
4. Enter a **Description** for the solution.
5. In **Object Types**, assign object types to the solution. Either add them by selecting a profile or add them individually, or both.
6. Click **Done**.

The solution displays in the solution schema visualization editor. For more information, see [“Using the solution schema visualization editor”](#) on page 250.

To change the object types that are assigned to the solution after it is created, click  in the Solution List. The Quick View panel opens and you can add and remove object types.

Property rendering JSP files

Every object type requires a property rendering JSP file. The JSP file controls the format of the elements that comprise the layout of a form on a Web page.

Note: This information applies only to Windows environments. For Linux environments, contact IBM OpenPages Support for assistance.

IBM OpenPages with Watson includes a generic property rendering JSP file, called `properties.jsp`, that is used by object types and cannot be changed. It is located in the `<OP_Home>|applications|op-apps|sosa|activityview` folder.

Where `<OP_Home>` is the installation location. By default, this location is `c:\OpenPages`.

Note: For backward compatibility with upgraded OpenPages systems prior to the 5.5 release, the existing JSP file, called `renderProperties.jsp`, is still used by the standard object definitions. This existing file, however, maps to the `properties.jsp` file.

For custom forms, you can either create your own custom property rendering JSP file or use the supplied `properties.jsp` file. If you choose to use the supplied JSP file for a custom form or survey, when the form or survey displays on a page, it will have the standard look and feel of an object page.

If you choose to create custom property rendering JSP files to use with your custom forms or surveys, it is best to create a "survey" folder under the `\sosa` folder path in which to store your custom JSP file or files. For example:

```
<OP_Home>\applications\op-apps\sosa\survey
```

For assistance in creating custom property rendering JSP files, see your OpenPages Managing Consultant.

When you create a new object type for a custom form, the path you provide for the JSP file will be relative to the `...\applications\op-apps\sosa` folder.

Accessing object types

From an object type, you can configure properties, such as which field groups should be included or excluded, associate parent and/or child object types, manage filters, dependent fields, and so forth.

Before you begin

Log on to IBM OpenPages with Watson as a user with the Object Types application permission set. For more information, see [“Types of application permissions” on page 91](#).

About this task

Object types can be managed using tasks in either the Task Focused UI or the Standard UI. Changes made in one interface are immediately reflected in the other. Functionality between the two user interfaces is mostly the same but there are a few exceptions. In the Task Focused UI:

- When you add a field, you can add it directly to all or a subset of profiles that the object type is assigned to. In the Standard UI, fields must be manually added to each profile.
- Display Type on fields is defined at the field level on object types. In the Standard UI, Display Type on fields is defined on fields at the profile level.

For more information about using the Task Focused UI to work with object types, see [“Working with object types \(Task Focused UI\)” on page 253](#).

For more information about using the Standard UI to work with object types, see [“Editing object type properties” on page 254](#) and numerous other topics.

Procedure

Click  > **Solution Configuration** > **Object Types**.

Or, in the Standard UI, click **Administration** > **Object Types**.

Working with object types (Task Focused UI)

From an object type in the Task Focused UI, you can add and edit fields, add and edit field groups, add and edit filters, and enable and disable relationships. You can also view profiles, views, and workflows.

About this task

Functionality for object types, fields, and field groups is parallel between the Task Focused UI and the Standard UI. In the Task Focused UI, functionality is centralized from the  > **Solution Configuration** > **Object Types** task.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Select **Show Profiles** to a view of a grid of all profile assignments on object types. The screen provides a helpful summary of profile assignments per object type. Changes to assignments should be made from profiles because from there you can more clearly view fields and filters and control what the change entails. For more information, see [“Creating a profile \(Task Focused UI\)”](#) on page 298.
3. Click an object type.
4. View information in the **General** section. Values in this section cannot be changed.
5. Expand the **Field Groups** section to add field groups to object types.
For more information, see [“Adding field groups to object types”](#) on page 207.
6. Expand the **Fields** section to create and work with fields and field groups.
For more information, see [“Defining fields and adding them to field groups”](#) on page 207.
7. Expand the **Relationships** section. View the parent and child object type associations in the **Parents** and **Children** sections. Select an object type and click **Enable** or **Disable** to change the association. Changes can be made from either the parent or the child object type. For more information, see [“Enabling associations between object types”](#) on page 256 and [“Disabling associations between object types”](#) on page 255.
8. Expand the **Profiles** section to work with profiles.
 - a) Click **Add**.
 - b) Select the box next to each profile to add to the object type.
 - c) Click **Done**.
9. Expand the **Filters** section to work with filters.
To create a filter, see [“Adding filters to object types \(Task Focused UI\)”](#) on page 271.
To edit a filter, open it, make your changes, and click **Done**.
10. Expand the **Views** section. View the views that are used for the object type.
11. Expand the **Workflows** section. View the workflows that are used for the object type.

Editing object type properties

You can edit the description of an object type and set whether to keep older versions of the object type. The JSP Path can be edited only for custom forms.

Restriction: Do not use characters defined in CJK Unified Ideographs EXTENSION-B on Unicode in the description field.

Procedure

1. With the Object Types application permission set, click **Administration** from the menu and click **Object Types**.
2. Click the name of the object type to modify.
3. Click **Edit**.
4. Make the necessary changes.
5. To save an older version of this object type, select the **Save older versions of this object type?** check box. If this box is not checked, the old version is overwritten.
6. Click **Save**.

Note: To change label text for an object type, see [Chapter 17, “Localizing text,”](#) on page 559.

Including field groups for an object type (Standard UI)

A new or existing field group must be added to an object type before any of the fields can be displayed on an object view page.

To create a new field group, see [“Adding field groups \(Standard UI\)” on page 223](#).

The object type can be predefined (see the topic, [“Platform object types” on page 249](#), for a list of object types) or a custom form.

Restriction: Before you can add a field group to a custom form or survey, create an object type for the custom form or survey. For information, see [“Adding an object type for a custom form” on page 265](#).

When you include a field group with an object type, the field group is displayed on the **Included Field Groups** tab of the object.

You can also exclude field groups from an object type if the field group is not marked as in use. Once an object of that type is created, or the field group is added to a type that already has existing object instances, you receive an error if you try to exclude the field group.

Before you begin

If you use IBM Db2 and the reporting schema is enabled, perform this task when there is limited or no activity on the system. It can cause significant system delays in OpenPages due to locking conflicts on the Db2 platform. For more information, see [“System delay when modifying object types and fields \(Db2\)” on page 1107](#).

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71](#).
2. With the Object Types application permission set, click **Administration** from the menu and click **Object Types**.
3. From the list, click the name of the object type.
4. On the **Included Field Groups** panel, click **Include**.
5. Select the field groups to include.
6. Click **Add**.

What to do next

To make fields visible to users in an object view, see [“Configure views for objects” on page 322](#)

Disabling associations between object types

If an association between a parent or child object type is no longer needed, disable the relationship between these object types.

For example, if a survey becomes obsolete and you no longer want it associated with a specific Risk object, disable the association between the survey object and the parent object type (SOXRisk).

For example, if you do not want users to associate certain object types together, such as Accounts with Business Entities, disable the association between the child object type (SOXAccount) and the parent object type (SOXBusEntity).

When you disable an association between object types, the following occurs:

- In the Task Focused UI, the child object type is marked as disabled in the **Relationships > Children** section on the parent object. The parent object type is marked as disabled in the **Relationships > Parents** section on the child object type.
- In the Standard UI:

- For objects, the child object type is removed from the Detail View page of the parent object. The parent object type removed from the Detail View of the child object type.
- For a custom form or survey, the custom form or survey is removed from the available form types that can be added from the **Associated Files and Forms** tab of a parent object.
- The **Disable** icon on the **Association Detail Info** page for the child object type changes to **Enable**.
- The value of the **Enabled** property changes from "true" to "false".
- The object type is removed from the Audit Trail page and Audit reports, even if the object type is a child for a different parent.
- The value of the setting is displayed as Read-only on the Child Association Detail Info page.

Before you begin

Ensure that your user has the Object Types application permission.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71.](#)
2. Click  > **Solution Configuration** > **Object Types**.
3. From the list, click the name of the object type to modify.
4. Expand the **Relationships** section. Object types are listed in two sections: **Parents** and **Children**.
5. Click the name of the object type to disable.
6. Click **Disable**. The icon in the **Enabled** column changes to an X.
7. To add the object relationship changes to reports, complete the following tasks:
 - a) Update the Reporting Schema. For details, see [“Creating or recreating the reporting schema \(Standard UI\)” on page 163.](#)
 - b) Regenerate the reporting framework. For details, see [“Updating the reporting framework \(Standard UI\)” on page 978.](#)

Enabling associations between object types

To allow an association between a parent or child object type that was disabled, enable the association between these object types.

When you enable an association between object types, the following events occur:

- In the Task Focused UI, the child object type is marked as enabled in the **Relationships > Children** section on the parent object. The parent object type is marked as enabled in the **Relationships > Parents** section on the child object type.
- In the Standard UI:
 - The enabled child object type displays on the Detail page of the parent object type.
 - The **Enable** icon changes to **Disable** on the Association Detail Info page.
 - The value of the **Enabled** property changes from "false" to "true" on the Child or Parent Associations tab.
 - The object type is included in the Audit Trail page and Audit reports
 - The value of the setting is displayed as Read-only on the Child Association Detail Info page.

Before you begin

Ensure that your user has the Object Types application permission.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71.](#)
2. Click  > **Solution Configuration** > **Object Types**.
3. From the list, click the name of the object type to modify.
4. Expand the **Relationships** section. Object types are listed in two sections: **Parents** and **Children**.
5. Click the name of the object type to enable.
6. Click **Enable**. The icon in the **Enabled** column changes to a check mark.
7. To add the object relationship changes to reports, complete the following tasks:
 - a) Update the Reporting Schema. For details, see [“Creating or recreating the reporting schema \(Standard UI\)” on page 163.](#)
 - b) Regenerate the reporting framework. For details, see [“Updating the reporting framework \(Standard UI\)” on page 978.](#)

Configuring OpenPages to associate a large number of child objects

If the number of associations that you add exceeds the maximum, the result is a long running process. The default is 250. This information applies only to child associations, not parent associations.

About this task

You can use IBM OpenPages with Watson to associate a large number of child objects by using the Add New Wizard as well as using the **Associate an existing issue** command from the **Actions** menu in the Detail view or Activity view. When the number of child associations exceeds the limit set in the **Max Child Associations Interactive** setting in the registry, the process runs in the background and you receive an email when it completes.

You might see something similar to the following message:

Due to the large number of associations, the objects will be associated in the background. You will receive an email when the process is complete.

These settings are set by default. You can change the following settings to specify the maximum number of associations, the timeout length, and the email response to a long running process.

Procedure

1. To specify the number of child objects to associate before background processing begins:
Applications > **Common** > **Configuration** > **Max Child Associations Interactive**. The default is 250.
2. To specify the transaction timeout for the background process, click **Platform** > **Processes** > **Associate Resources** > **Transaction Timeout**. The default is 21600 seconds.
To show the **Transaction Timeout** setting, change the value of **Applications** > **Common** > **Configuration** > **Show Hidden Settings** from false to true. The default value is false.
3. To specify the email settings for the email server configuration, click:
 - **Applications** > **Common** > **Email** > **Mail Server**
 - **Applications** > **Common** > **Email** > **SMTP Password**
 - **Applications** > **Common** > **Email** > **SMTP Port**
 - **Applications** > **Common** > **Email** > **SMTP Security Type**
 - **Applications** > **Common** > **Email** > **SMTP User Name**
4. Optional: You can customize the email subject and content. From the menu bar, click **Administration** > **Applications** > **Application Text** > **Miscellaneous**.

- `com.resource.association.email.subject.success`
- `com.resource.association.email.subject.warning`
- `com.resource.association.email.subject.error`
- `com.resource.association.email.content.success`
- `com.resource.association.email.content.warning`
- `com.resource.association.email.content.error`

Object relationship types

The relationship type between object types in the object model can be either Association (parent-child) or Reference (non-parent-child).

The Association relationship type is the most common relationship. It defines parent and child relationships between object types in the object hierarchy.

The Reference relationship type is used for non-parent-child relationships. This relationship type is not traversed when navigating the hierarchy. It is used to avoid loops or cyclic relationships in the object model.

Let's say that in your business model a relationship exists between SubAccount objects and Process objects. The following diagram demonstrates how a path from SubAccount to Process in an object model can create a loop or cyclic relationship if the relationship type is defined as Association. Starting at Entity, as you traverse the hierarchy through the parent-child relationships, you enter a loop between SubAccount and Process. This is an invalid configuration.

Types of relationships

- Parent-Child Association
- Reference

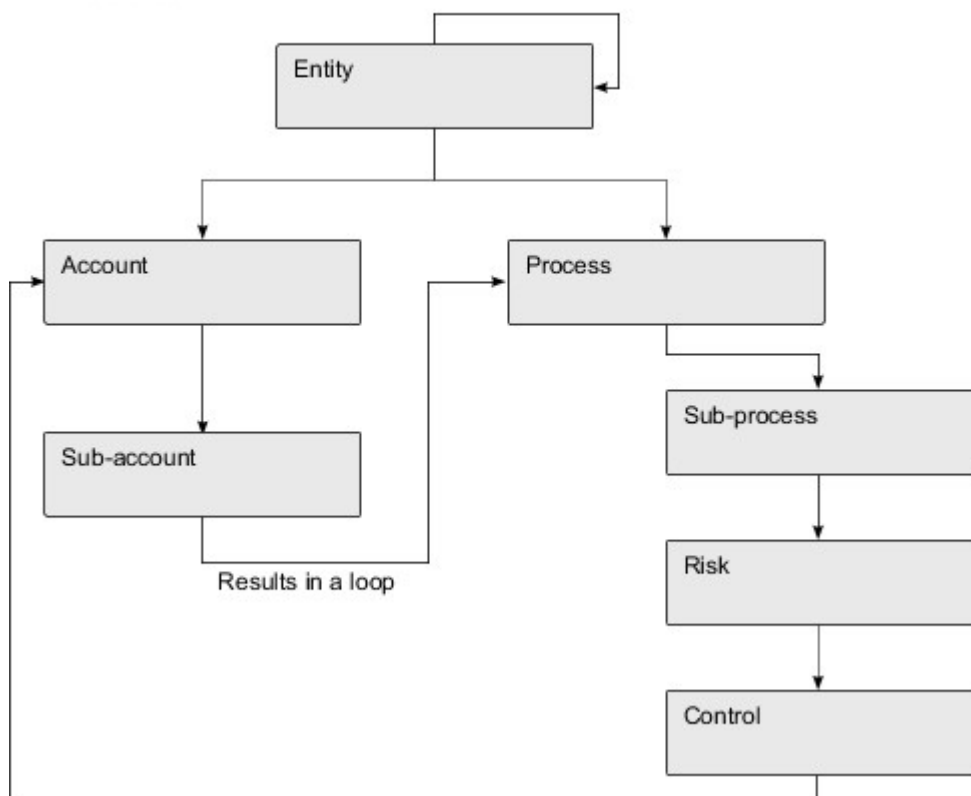


Figure 14. Sample invalid cyclic relationship

There are two methods to avoid such a loop between objects in the hierarchy:

- Disable the relationship that creates the loop. For example, if the relationship defined in the object model is not being used (that is, there exists no instance data in your database that has these relationships), disable the relationship. For details, see [“Disabling associations between object types”](#) on page 255.
- Leave the relationship that creates the loop, but change its type to Reference. Use this option if, for example, the relationship that creates a loop accurately describes your business model, as in [Figure 15 on page 259](#). For details on changing the reference type, see [“Setting the relationship type”](#) on page 259.

[Figure 15 on page 259](#) illustrates how a valid relationship between SubAccount and Process can be maintained without a loop by setting the Relationship Type between these objects to Reference.

Types of relationships

- Parent-Child Association
- Reference

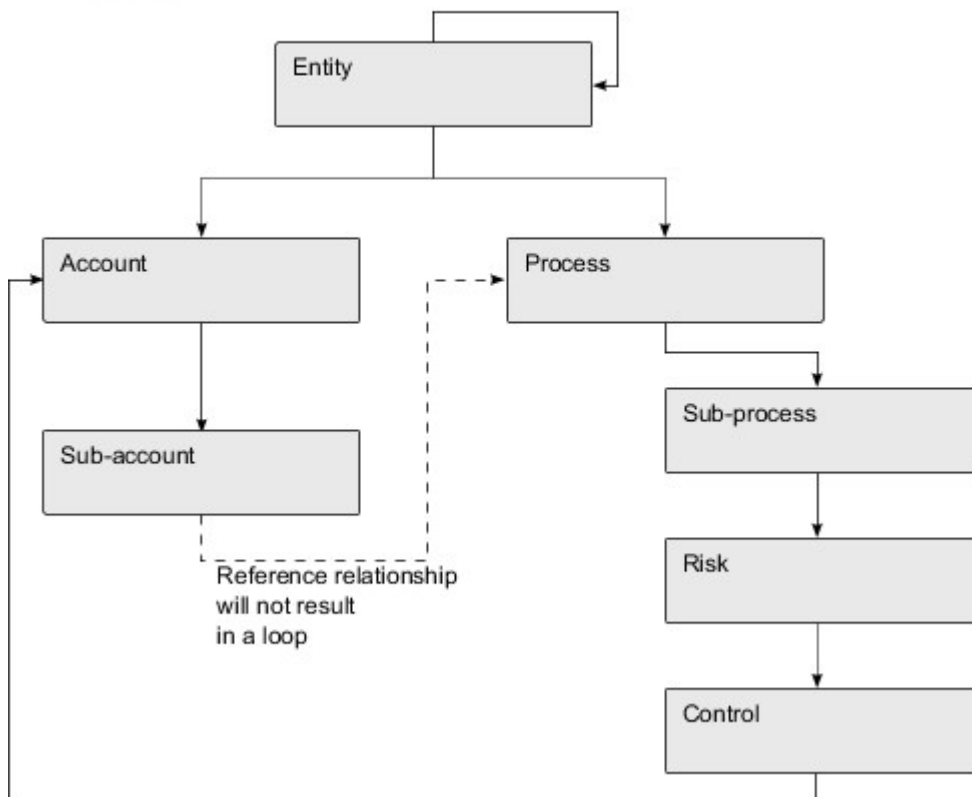


Figure 15. Sample reference relationship

Setting the relationship type

You can set the relationship type between object types.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode”](#) on page 71.
2. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
3. Click the name of the parent object type with the child relationship to modify.
4. On the **Child Associations** panel, select the child object to modify.
5. Click **Edit**.
6. Select a value in the **Relationship Type** field. Valid values are:

- Association
- Reference

For more information about the relationship types, see [“Object relationship types”](#) on page 258.

7. Click **Save**.

Configure the ability to create a draft copy of an Object (Standard UI)

Configure the Save As Draft feature to display a **Save As Draft** icon when the user edits or creates objects. Users can save object data without completing all required fields.

The **Save As Draft** icon is displayed next to the **Save** icon on the **Detail View** page of an object type when the object is in edit mode.

To configure the Save As Draft option, create a field group and an enumerated string field. After the group and field are created, use these values to enable the **Save As Draft** icon. The group and field can then be associated with object types in a profile. The field does not have to be associated with a view in a profile to display the **Save As Draft** icon.

See the following topics for details on the Save As Draft configuration process:

- [“Creating a field group and field for a Save As Draft configuration”](#) on page 260
- [“Configure the Save As Draft feature for new objects”](#) on page 261
- [“Adding the field to the object type and profile to configure the Save As Draft function ”](#) on page 261

In the illustration, the field group in the [“Creating a field group and field for a Save As Draft configuration”](#) on page 260 procedure is called "DraftGroup" and the enumerated field is called "Draft Status" with values of "Draft" and "Published".

When the user clicks **Save As Draft**, the value of the **Draft Status** field is automatically set to "Draft". When the user clicks **Save**, the required fields are automatically validated and the value of the **Draft Status** field is set to "Published". It is best to hide the "Draft Status" field from object views in a profile. However, if you make the "Draft Status" field visible in a profile object view, configure it as Read only.

Use the Save As Draft feature with Activity View pages

To use the Save As Draft feature with **Activity View** pages, the **Save As Draft** icon must be configured on the root or parent object type. The root or parent object is the first object type that is listed in the Activity View.

If a child object type has **Save As Draft** configured but the parent object type does not, **Save As Draft** is not visible on the **Activity View** page.

The required field validation is skipped on child objects if they have the draft field in the profile. Required field validation on the child object is completed if no draft field is defined in the profile, even when a user click **Save as Draft**.

Creating a field group and field for a Save As Draft configuration

To add a Save As Draft icon to an object view, you first create a field group and field.

Before you begin

Complete the following steps to create a field group and add field definitions to the group:

Procedure

1. Create a field group and name it. See [“Adding field groups \(Standard UI\)”](#) on page 223.
2. Add a field definition to the new field group and name it.

- a) Select the **Enumerated String** data type.
- b) Add a value for Draft and a value for Published . See [“Adding fields to a field group \(Standard UI\)” on page 223.](#)

Related tasks

[“Configure the Save As Draft feature for new objects” on page 261](#)

[“Adding the field to the object type and profile to configure the Save As Draft function ” on page 261](#)

Configure the Save As Draft feature for new objects

To configure the Save As Draft feature, the second task is to configure settings.

Before you begin

Complete the following steps to configure settings:

Procedure

1. From the configuration folder, click **Show Hidden Settings**. Set the value to true. For more information, see [“Show hidden settings” on page 602.](#)
2. Expand the **Common | Configuration | Required Field Validation** folder hierarchy.
3. Select **Draft Status Field**. In the **Value** field, type the name of the field group and the field. click **Save**. The format is <field group>.<field name>. For example, typeDraftGroup.Draft Status.
4. Click **Draft Status Value**. In the **Value** field, type the system name of the draft value and click **Save**. For example, typeDraft
5. Click **Publish Status Value**. In the **Value** field, type the system name of the draft value. For example, type Publish.

Related tasks

[“Creating a field group and field for a Save As Draft configuration” on page 260](#)

[“Adding the field to the object type and profile to configure the Save As Draft function ” on page 261](#)

Adding the field to the object type and profile to configure the Save As Draft function

The third task in the Save As Draft configuration is to add the new field to the object type and profile.

Procedure

1. Enable System Admin Mode. Click  > **Enable System Admin Mode**. For more information, see [“Enabling and disabling System Admin Mode” on page 71.](#)
2. For each object type to enable the **Save As Draft** icon, include the new field group. For example, include the field group called DraftGroup. See [“Including field groups for an object type \(Standard UI\)” on page 255.](#)
3. Disable System Admin Mode. Click  > **Disable System Admin Mode**.
4. Include the new field. For example, include the field that is called Draft Status, in a profile. See [“Including fields in an object type” on page 306.](#)

Note: Unless you want the field to be visible to users, the field does not have to be included on a **View** page for **Save As Draft** to be displayed.

Related tasks

[“Creating a field group and field for a Save As Draft configuration” on page 260](#)

[“Configure the Save As Draft feature for new objects” on page 261](#)

Stand-alone object settings

Cardinality settings determine if an object can be created as a standalone object and whether it can be associated with more than one parent object.

Important: The setting values control the options on the user interface that allow users to create objects as stand-alone. The setting values are NOT currently used to enforce the number of associations between object instances.

In new installations, the default values for the minimum (Min Children = 0) and maximum (Max Children = 2147483647) number of children should not be modified.

Enabling the creation of stand-alone objects

When a user adds a child object type from the **Detail** page of a parent object type, the child object type is created and associated with the parent object type. A stand-alone object is a child object that is not associated with a parent object.

For example, if you select **Risks** on the **Assessments** menu, and then click **Add New** on the Risk **Folder View** page, a child object is created in the top-level Risk object type folder but is not be associated with a parent object.

You control the ability of users to create standalone object types by configuring the value of the minimum parents cardinality setting.

If the value of the minimum parents cardinality setting, **Min Parents**, is set to:

- **0 - Add New** is displayed on the object **Folder View** page. Users can create stand-alone instances of a child object type. If a child object type has multiple parent relationships, the value of **Min Parents** must be set to zero for every relationship in which that object type is a child. You cannot create stand-alone objects from a Detail View or Activity View page.
- **1 - Add New** is removed from the object **Folder View** page. Users cannot create stand-alone instances of a child object type. This value is the default setting in new installations.

Note: For data consistency, set the minimum parent setting to either 0 or 1. A minimum parent setting that is greater than 1 is the same as setting it to 1.

Procedure

1. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. Click the name of the object type to modify.
3. On the **Parent Associations** panel, click the name of a parent object type.
4. On the **Association Detail Info** panel, click **Edit**.
5. In the **Min Parents** box, type 0 (for standalone) or 1 (to prevent a stand-alone object type).
6. Click **Save**.
7. For multiple parent objects, repeat Steps 3 - 6 for each parent object.

Enabling the ability to associate objects

For object type relationships that contain a child object type, you can control the ability of users to associate child object types. Control them by configuring the value of the maximum parents cardinality setting.

Use the following information to determine the value to set in the maximum parents cardinality setting (**Max Parents**):

- 2147483647 (infinity) in the **Max Parents** field enables the display of the **Associate** and **Disassociate** menu items on the **Detail** view of the object type. Users can associate that object to more than one parent object. The default value is 2147483647.

- 1 in the **Max Parents** field removes **Associate** and **Disassociate** menu items from **Detail** view of the object type. Users cannot create shared instances of a child object type.

Notice: The maximum parents associations on a child object is not enforced. For instance, if the maximum parents setting is 2, the application allows a child object to be shared among 3 or more parent objects of the same type. A maximum parent setting of greater than 2 is the same as setting it to infinity.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
2. From the list, click the name of the parent object type whose child relationships you want to modify.
3. On the **Child Associations** tab, click the name of the child object type you want to modify.
4. On the **Association Detail Info** tab, click **Edit**.
5. In the **Max Parents** box, enter 2147483647 (for shared) or 1 (for not shared).
6. Click **Save**.
7. If you more than one child objects for which you want to restrict the parent object relationship, repeat Steps 3 - 6 for each child object.

File type information

A file type describes the structure or format of a file and is typically reflected in the file name extension.

Some common examples of file name extensions include .rtf (Rich Text Format), .txt (ASCII text), .doc (Microsoft Word), .pdf (Portable Document Format), .xls (Microsoft Excel), .htm (Hypertext Markup Language), and .jsp (Java Server Page).

In IBM OpenPages with Watson file type extensions are case sensitive.

Note: Only the SOXDocument object type supports file types.

Each file type has a corresponding MIME (Multipurpose Internet Mail Extension) type associated with it, which is a standardized data exchange method used by Web browsers to associate files with helper applications that display files of that type. For example, a MIME type of image/gif, informs the browser to handle the data as an image. The IBM OpenPages with Watson application supplies a number of predefined MIME types.

Adding a file type

When you add a file type to the application, it is automatically added to the File Type Information selection list.

Before you add a file type, verify that it does not already exist. To view a list of file types, click **Include** on the **File Types Information** panel of the SOXDocument object type. If the file type is displayed in the list, go to [“Associating a file type with an object type” on page 264](#). If the file type is not displayed, click **Cancel** and complete this procedure.

In IBM OpenPages with Watson file type extensions are case sensitive.

Procedure

1. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. Click **SOXDocument**.
3. On the **File Types Information** panel, click **Add New**.
4. In the **MIME Type** field, type a MIME content type and subtype. For example, image/cgm.
5. In the File Extension field, type a file extension that corresponds to the MIME Type. For example, cgm.
6. Click **Create**.

What to do next

To associate the new file type with the SOXDocument object type, see [“Associating a file type with an object type”](#) on page 264.

Associating a file type with an object type

You can associate various file types with the SOXDocument object type. If you have added a new file type, you will need to associate it with the object type before it can be used.

Note: When you attach a file to an object, the file extension is case sensitive and must match the extension specified in the File Types Information section of the SOXDocument object type.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
2. From the list, click the **SOXDocument** object type.
3. On the **File Types Information** tab, click **Include**.
4. From the list on the **Select File Type Information** page:
 - a) Select the check box next to the name and MIME type you want to add. You can select multiple boxes.
 - b) When finished, scroll down and click **Add**.
The newly associated file type is listed on the **File Types Information** tab of the SOXDocument object type.

Removing a file type from an object type

You can remove a file type from the SOXDocument object type if file type is not in use. Removing a file type from an object type does not remove the file type from the File Type Information selection list.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
2. From the list, click the **SOXDocument** object type.
3. On the **File Types Information** tab:
 - a) Select the check box next to the name and MIME type you want to remove.
 - b) Click **Exclude**.

Results

The associated file type is removed from the list on the **File Types Information** tab of the SOXDocument object type.

Note: Files might still be discovered after the extension of these files is excluded from search. If a file extension is associated with more than one MIME type, then files with this extension are still discovered until all associated MIME types are excluded or are disabled from search. Follow the procedure [“Removing a file type from other object types”](#) on page 264 with each associated MIME type to remove the types from searches. For more information, see [“Enabling attachment file types for global search”](#) on page 654.

Removing a file type from other object types

You can remove a file type if a file extension is associated with more than one MIME type..

Procedure

1. Move the MIME type from the exclusion list to the inclusion list.
2. Disable the MIME type.
3. Move the MIME type back to the exclusion list.
4. Run the **Update** command.

For more information, see [“Enabling or disabling object types or fields for global search” on page 655](#).

Tasks required to set up custom forms

To set up custom forms, such as surveys, you must complete many tasks.

Note: If you imported a custom form through the ObjectManager, perform Task 6.

Table 102. Tasks for adding custom forms	
Task Description	Related Topic
1. Create an object type for the custom form.	See “Adding an object type for a custom form” on page 265 for step-by-step instructions on how to create an object type for a custom form.
2. Add a field group for the custom form object fields.	See “Adding field groups (Standard UI)” on page 223 for step-by-step instructions on how to create one or more field groups that will contain the fields for the custom form.
3. Add one or more field definitions to the new field group.	See “Adding fields to a field group (Standard UI)” on page 223 for instructions on how to add new field definitions to a new field group.
4. Add the new field group to the custom form object type.	See “Including field groups for an object type (Standard UI)” on page 255 for information about how to add the new field group to a custom form object type so the fields can be available for display.
5. Associate the custom form object type with a parent object type.	See “Associating a custom form from a parent object” on page 266 for information about how to associate a child object type (custom form) with a parent object type.
6. Include the new custom form object type in a profile.	See “Including object types in a profile” on page 304 for information about how to include the custom form object type on an object’s view page.
7. To run reports against a custom object type, specify a custom prefix for the real-time reporting schema tables.	See “Enabling the reporting framework for custom forms” on page 960 for information about adding a custom prefix.

Adding an object type for a custom form

If you want to add a custom form, such as a survey, to an object, you must first create an object type for that custom form. After the object type is created, you can include field groups and associate parent objects to it.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71.](#)
2. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
3. On the **Object Types** pane, click **Add**.
4. On the add page, complete the following steps:
 - a) Type a name for the new object type.

The name must start with a letter, and can only contain letters, numbers, and the underscore (_) character. The name is also used as the initial label for the object type and cannot be modified after it is created.

Examples include:

```
RiskSurvey, survey1, Survey1_Risk
```
 - b) In the **JSP Path** field, type the folder path and name of the .jsp file that will be used by the object type to render the layout and presentation of the object on the Web application page. The default path is /propertyForm/renderProperties.jsp.

Note: The path of the JSP file is relative to the <OP_HOME>/wlp-usr/shared/apps/op-apps.ear/sosa.war/ directory.
If you are using, for example, a custom JSP file, the folder and file name might look similar to this: /Survey/MySurvey.jsp.
 - c) Click **Create**.

The object type is created, and the Object Type detail page displays where you can configure properties. For details see, [“Editing object type properties” on page 254.](#)
5. To run reports against this custom object type, you must configure a custom prefix for the real-time reporting schema tables. For details, see [“Enabling the reporting framework for custom forms” on page 960.](#)

Deleting a custom object type

You can only delete custom object types that are not in use in the application.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71.](#)
2. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
3. Select the object type to delete..
4. On the **Object Types** tab, click **Delete**.

Associating a custom form from a parent object

You can only add child object associations to object types; you cannot add child associations to a custom form or survey object types from the Detail page of a parent object.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71.](#)
2. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.

3. Click the name of the object type to modify.
4. On the **Child Associations** tab, click **Add**.
5. On the **Available Custom Forms** page, select each custom form to associate with the selected parent object type.
6. Click **Add**.

Associating a custom form to a parent object

You can only add parent object associations to a custom form or survey object types; you cannot add new parent object associations to an object type from the Details page of a custom form object.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71](#).
2. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
3. Click the name of the custom form object you want to modify.
4. On the **Parent Associations** tab, click **Add**.
5. On the **Available Object Types** page, select each parent object where the object type will be attached.
6. Click **Add**.

Tasks to define filters for an object type

Filters are specific to an object type and are used to narrow the scope of data that is returned in a view for that object type.

When you create a filter for an object type, you can select which fields to use to search for data. Only the objects that match the specified search criteria are returned for that object type.

Filters that are created by administrators are also called public filters. Public filters are usable by any user who has them in their profile. Users can also create their own private filters.

Filters can be defined in either the Task Focused UI or the Standard UI. In the Task Focused UI, functionality is centralized from the  > **Solution Configuration** > **Object Types** task.

In the Task Focused UI, filters are used in views, workflows, dashboard panels, charts, and more.

In the Standard UI, filters are used with Filtered List Views, Grid Views, Activity Views, and the Home page. An object type can have multiple filters.

The following table provides an overview of the flow of tasks for adding filters to object types and views.

<i>Table 103. Tasks for configuring filters and views</i>		
Task	Task Description	Related Topic
1	Determine the purpose and characteristics of the filter.	“Filter considerations” on page 268
2	Add the filter to an object type.	“Adding filters to object types (Task Focused UI)” on page 271 “Adding filters to object types (Standard UI)” on page 273
3	Add localized names for the filter (optional)	“Modifying object text (Task Focused UI)” on page 561

Table 103. Tasks for configuring filters and views (continued)		
Task	Task Description	Related Topic
3	Apply the filter in various places, for example, views.	

Filter considerations

Before you create a filter, determine the characteristics of the filter and identify the object type on which the new filter is used.

For instructions on creating a filter, see [“Adding filters to object types \(Task Focused UI\)” on page 271](#) and [“Adding filters to object types \(Standard UI\)” on page 273](#).

The following list identifies information that you need before you create a new filter:

- Object type - Which object type will the filter be used with?
- Name - How will the new filter be identified? The name of the filter is important because it is also the initial label that will appear for the filter in the application.
- Profiles - Which profiles will be associated with the filter?
- Filtering criteria - Which fields are used in the filter criteria to narrow the scope of data returned by the search?
- Views, dashboard panels, and more - Where is the filter needed in the Task Focused UI?
- Localization - Does the filter name need to be localized? If so, the translated names are defined by using object text. For more information, see [“Modifying object text \(Task Focused UI\)” on page 561](#).
- Views - Which type of view page in the Standard UI will use the filter (Grid View, Filtered List View, Home page, Activity View)?

Example

You create a filter for risk assessments called "In Progress" that displays all risk assessments due within the next three months, and has the following selected fields and values:

Table 104. Sample risk assessments fields	
Field	Value
Status	In Progress
Start Date	On this date
End Date	In the next 90 days

Uses in the Task Focused UI

If you associate this filter to the "Assessors" profile, application users who are assigned the Assessors profile would then be able to select this filter in various places. For example, if they create a dashboard panel, chart, or Grid View for the for Risk Assessment object type, they can apply the filter.

Uses in the Standard UI

If you associate this filter to a Filtered List View in the "Assessors" profile, application users who are assigned the Assessors profile would then be able to select this filter from the Risk Assessment Filtered List View filter selection list and from any Risk Assessment Grid View for that profile.

You could also create a personalized "My In-Progress Risk Assessments" filter for use on the Home page from the "In Progress" filter. You would do this by making a copy (see [“Copying filters \(Standard UI\)” on page 276](#)) of the "In Progress" filter, renaming it to "My In-Progress Risk Assessments", and selecting "End User" as the Assessor. When you configure the "My In-Progress Risk Assessments" filter for the

Home page, application users who were assigned the "Assessors" profile would only see their assigned risk assessments that were due within the next 3 months on their Home page.

Filters that contain unavailable fields

When a filter contains a field that is no longer available (for example, the field was excluded from a profile), when that filter is selected, the row with the unavailable field is replaced by the default filter condition.

To resolve this issue, edit the filter to remove the unavailable field.

Limitations on special characters in filters for long string fields

When you create filters for long string fields, some special characters have limitations on how they are used.

Do not use special characters as first or last character

When you use a filter to search for text in long string fields, the following special characters and symbols might not return the expected results if these characters are the first or last character in the text to be searched:

- Characters in languages such as Chinese, Japanese, and Thai.
- Some three-byte Unicode characters and symbols such as * № € Å ☆ @

Note: When you search for text that contains these special characters, you must use the **Contains** search condition in the filter.

For example, you want to search for text that has the phrase "maximum € 120". For the selected text field, you would choose the **Contains** search condition, and type the words: maximum € 120.

The search results would return the following: "The maximum € 120 is the upper limit" because the special character appears in the middle of the text and not at either the beginning or end.

The search results would NOT include the following: "€ 120 is the maximum upper limit" or "The maximum upper limit is 120 €" because the special character is the first or last character in the text.

Important: You can use the forward slash to create filters for folders. If you want to start or end your filter with a forward slash, then you must use a double forward slash. The first forward slash is stripped out. For example, if you enter a folder, enter it as //foldername.

Reserved characters

Table 105. Reserved characters that have special meaning in the filters	
Reserved character	Description
_	An underscore is used as a single character wildcard.
%	A percent sign is used as a multiple character wildcard.

Do not use these special characters

The following special characters are not validated in neither the Task Focused UI nor the Standard UI.

Table 106. Special characters that are not supported in search filters	
Special Character	Description
&	Ampersand

Table 106. Special characters that are not supported in search filters (continued)

Special Character	Description
@	At symbol on keyboard
!	Exclamation point or bang
\	Backward slash
^	Caret or circumflex
:	Colon
;	Semicolon
,	Comma
-	Dash
>	Greater than sign
<	Less than sign
(	Opening parenthesis
)	Closing parenthesis
=	Equal sign
	Pipe or vertical bar
+	Plus sign
#	Pound or number sign, hash symbol
?	Question mark
~	Tilde or equivalency sign
`	Grave accent
[	Opening bracket
]	Closing bracket
{	Opening brace
}	Closing brace
\$	Dollar sign
¥	Yen sign
₩	Won sign
ᄅ	Yi syllable IT
	Double vertical lines

The following reserved words are not supported in the search filter and should not be used:

- ABOUT
- ACCUM
- AND
- BT

- BTG
- BTI
- EQUIV
- FUZZY
- HASPATH
- INPATH
- MDATA
- MINUS
- NEAR
- NOT
- NT
- NTG
- NTI
- NTP
- OR
- PT
- RT
- SQE
- SYN
- TR
- TRSYN
- TT
- WITHIN

Note: Reserved words are not case-sensitive.

Adding filters to object types (Task Focused UI)

Filters are specific to an object type and narrow the scope of data that is returned in a view for the object type. When you create a filter for an object type, select which fields to use to search for data. Only the objects that match the specified search criteria will be returned for that object type.

For up-to-date results of filters that include long string fields, the text index for the long string field must have been synchronized with the values in the field. Synchronization depends on when the index was created or the setting of scheduled synchronization. For details on the index creation and synchronization utilities provided for long string filtering, see [“Utilities for filtering on long string field content in an Oracle database” on page 746](#).

Note: If you create a new filter that uses the character % as the value, for example Name Contains %2, the Name Contains value field appears empty after you load the filter: the % character does not appear. However, the filter runs properly.

Before you begin

Log on with a user that has the Object Types application permission.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Click an object type.
3. Expand the **Filters** section to work with public filters.

4. Click **New Filter**.
5. Enter a **Name**.
6. Enter a **Description**.
7. Click **Add** to define a condition.
 - a) Select a **Field**.
 - b) Select an **Operation**. The available operations and remaining fields depend on the field you selected.
 - c) Complete the remaining fields.
For example, for a name field, the options are **Starts with**, **Contains**, and **Equals** and a text value.

Note: Text is not case sensitive.

<i>Table 107. Search conditions</i>	
If a condition field is a	You can do this
A user	Select the Matches the selected user operation and add one or more users in the list under Other user . Or, you can set End User to resolve to the currently logged-on user.
A group	Select the Includes all of the selected users operation and add one or more groups in the list under Other group . Or, you can set End User to resolve to the currently logged-on user.
An enumerated value	Select the Any of the following values operation and add enumerated values in the list under Select Values . You can also set Show hidden values .
An alphanumeric value	Select an operation (such as Starts with , Contains , Equals , and Ends with) and then enter a value.
A date	Select an operation (such as In the last , In the next , On a specific date , and In the range) and then enter a value.
A numeric value	Select an operation (such as Equals , Greater than , Less than , and In the range) and then enter a value.
A Boolean	Click true or false .

Important: For limitations on the special characters in filters for long string fields, see [“Limitations on special characters in filters for long string fields”](#) on page 269.

- d) Click **Done**.
- e) Optional: Add more conditions.
- f) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

For details on specifying more complex logic for your filters, see [“Using complex logic in a search filter \(Standard UI\)”](#) on page 274.

8. Expand **Profiles** and assign the filter to one or more profiles.

Although a profile is not required, a filter must be assigned to a profile to be available to use.

9. Click **Done**.

What to do next

If the filter name must be localized, see [“Modifying object text \(Task Focused UI\)”](#) on page 561.

Adding filters to object types (Standard UI)

Filters are specific to an object type and narrow the scope of data that is returned in a view for the object type. When you create a filter for an object type, select which fields to use to search for data. Only the objects that match the specified search criteria will be returned for that object type.

For up-to-date results of filters that include long string fields, the text index for the long string field must have been synchronized with the values in the field. Synchronization depends on when the index was created or the setting of scheduled synchronization. For details on the index creation and synchronization utilities provided for long string filtering, see [“Utilities for filtering on long string field content in an Oracle database”](#) on page 746.



Attention: If you create a new filter that uses the character % as the value, for example Name Contains %2, the Name Contains value field appears empty after you load the filter: the % character does not appear. However, the filter runs properly.

Procedure

1. Access the **Object Types** page (see [“Accessing object types”](#) on page 253).
2. From the list, click the name of the object type you want to modify.
3. On the **Filters** tab of the selected object type, click the plus sign icon.
4. On the **Add Filter** page:

- a) Click the **Field** field and select a key field from the list.

Common fields are listed first, followed by fields specific to the object type.

- b) In the same row as the key field, specify a search condition.

The available search conditions change depending on the selected field. For example, for a name field, the options are **Starts with**, **Contains**, and **Equals**, with a following text box in which to enter a value.

Note: Text is not case sensitive.

Table 108. Search conditions	
If a field has a	You can do this
 user icon	Click to select a user from a phonebook. You can also select multiple users.
 group icon	Click to select a group from a hierarchical tree structure. You can also select multiple groups.
 search icon	Click to search for a user or group.

Table 108. Search conditions (continued)	
If a field has a	You can do this
End User link	Click to insert "End User" into the value. The value "End User" will resolve to the currently logged-on user. For details on the currently logged in user, see “Filtering on the currently logged on user (Standard UI)” on page 276
Select Values link	Select from a list of values.
Text box for alphanumeric values	Select a search condition (such as Starts with) and then enter a value.
 calendar icon or a text box for date ranges.	Click the calendar icon to select specific dates, or select a search condition (such as Within the last) and then enter a value.
Text box for numeric values (used in computed fields)	Select a search condition (such as =) and then enter a value.
	Click the true or false .

Important: For limitations on the special characters in filters for long string fields, see [“Limitations on special characters in filters for long string fields” on page 269](#).

- c) To add another row and key field on which to search, click the **Add** link and repeat step 4.

By default, all the rows are connected (by their sequential number) with an AND operator (for example 1 AND 2 AND 3). That is, all of the conditions specified must be true.

For details on specifying more complex logic for your filters, see [“Using complex logic in a search filter \(Standard UI\)” on page 274](#).

- d) Click **Save**.

- To associated the filter with a view, see [“Tasks to associate filters with views \(Standard UI\)” on page 275](#).
- To create a duplicate filter using the new filter as a template, see [“Copying filters \(Standard UI\)” on page 276](#)
- To localize the display name of a filter, see [“Modifying display text for public filters \(Standard UI\)” on page 563](#).

Using complex logic in a search filter (Standard UI)

You can add complex logic to filters to help refine searches using logical operators such as OR, NOT, and parentheses. By default, the system uses only the AND operator to return results from a filtered search.

When you create a filter (see [“Adding filters to object types \(Standard UI\)” on page 273](#)) you select object fields and define the search criteria for each selected field. These key fields are then used by the system to search the database for objects that meet the specified criteria.

Every key field that is selected in a filter is displayed in a row that is sequentially numbered. This number of the row is its identifier. For example, the first key search field is displayed in row number 1, the next key search field is in row number 2, the next one in row number 3, and so forth. You use the row identifier with a logical operator to create a complex logic search expression. Although row identifiers are sequential, the identifier can appear in any order within the expression.

Use the logical operators described in the following table to define filtered searches. The operators are not case sensitive.

Table 109. Logical operators for complex logic

Operator	Purpose	Example
AND	Narrow the search for objects that meet all the search criteria. This is the default operator used to return results from a search filter.	1 AND 2 AND 3
OR	Broaden the search for objects that meet one or the other key search criteria.	1 OR 2 OR 3
NOT	Narrow the search for objects by excluding the specified key search criteria.	1 AND NOT 2
()	Group search criteria together to show the order in which the query should be applied.	1 AND (2 OR 3)

Procedure

1. In a **Filter** window (adding or editing a filter), click **Use Complex Logic**.
2. In the **Logic** text box, modify the search expression as wanted using the logical operators.
To close the **Logic** text box and revert to the default search logic, click **Clear Complex Logic**.
3. Click **Save** or select from **Actions** menu.

Examples

- You have 3 search fields defined in your filter. By default, the system uses only the AND operator so it would retrieve objects that only matched all 3 fields (1 AND 2 AND 3). If, however, you wanted to broaden the search so it included field 1 and either fields 2 or 3, use the OR operator to modify the search to retrieve all objects that matched field 1 and matched either fields 2 or 3.

To do this, create the logical expression: 1 AND (2 OR 3).

- You want to find open Issue objects that are not assigned to you. To create such a filter, you would select the "Issue Status" field and choose the "Open" value (this is field 1). Then select the "Assignee" field and choose your name from the **Select the user** window or click the **End User** link (this is field 2).

To exclude your name from the search results, in the **Logic** text box, you would type 1 AND NOT 2.

Note: The NOT operator does not return objects that have an empty, blank, or null value in the selected field criteria. This means that any unassigned Issue objects (that is, the "Assignee" field was empty or blank), would be excluded from the search results.

Tasks to associate filters with views (Standard UI)

After you create a filter for an object type, you can associate it to a profile and an object view.

Table 110. Associating filters procedures

Filter tasks	Procedure
Display the filter for selection by application users in the filters list under 'Public filters' on a Filtered List View page for an object type.	"Associating filters to Filtered List view and Grid view pages" on page 334
Use the filter to personalize the home page for users who are assigned a particular profile.	"Configuring filtered lists on the My Work tab" on page 315
Use the filter in an Activity View page to limit the scope of listed child objects.	"The layout of Activity views" on page 340 or "Modifying an Activity view" on page 343

Table 110. Associating filters procedures (continued)

Filter tasks	Procedure
Use the filter in a Grid View page to limit the scope of listed child objects.	“Creating a Grid view ” on page 335

Filtering on the currently logged on user (Standard UI)

You can create a filter that scopes the search to the currently logged on user for specific object type fields, such as Process Owner or Control Owner.

Procedure

Complete one of the following actions:

- Change the display type of the field from "Text" to one of the following display type options:

- User Selector
- User Dropdown
- User/Group Selector
- Group Selector

and then click the **End User** link. The End User value that is displayed in the box will resolve to the currently logged-on user. For details on modifying a display type for a field, see [“Configuring display types for simple string fields \(Standard UI\)” on page 349](#).

- Multi User Selector
- Multi Group Selector
- Multi User/Group Selector

- Type the following code into the text box of the object-specific field:

```
##{logged in user}##
```

Copying filters (Standard UI)

You can save an existing filter with a new name to use as a template.

Note: Because filters contain object-specific fields, you can only copy filters within the same Object type; you cannot copy filters between Object types.

Procedure

- With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
- From the list, click the name of the Object type to modify.
- On the **Filters** panel, click the filter you want to copy.
The **Edit** window opens for the filter.
- Select **Save as** from the **Actions** menu.
- Type a unique name (required) for the new filter. Click **Apply**.

Results

The new filter is now available in the **Filters** tab. For instructions on specifying filters and using complex logic in filters, see [“Adding filters to object types \(Standard UI\)” on page 273](#) and [“Using complex logic in a search filter \(Standard UI\)” on page 274](#).

To display the new filter in the list of Saved Filters on an **Filtered List View** page, add it to a profile. For details, see [“Associating filters to Filtered List view and Grid view pages” on page 334.](#)

Modifying filters (Standard UI)

After you create a filter, you can modify it. The modifications, once saved, are immediately used in the application.

Procedure

1. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. Click the name of the Object type to modify.
3. On the **Filters** pane, click the filter to edit.
4. Make the required changes.
 - To rename a filter, click **Actions > Rename**. Enter the new name and description and click **Apply**.
 - To change the filter or the complex logic, make the changes and click **Save**. For more information, see [“Adding filters to object types \(Standard UI\)” on page 273](#) and [“Using complex logic in a search filter \(Standard UI\)” on page 274.](#)

Results

To modify a localized display name of a filter, see [“Modifying display text for public filters \(Standard UI\)” on page 563](#)

To display the filter in the list of Saved Filters on an object’s Filtered List View page, add it to a profile. For details, see [“Associating filters to Filtered List view and Grid view pages” on page 334.](#)

What to do next

If you renamed the filter, there is an extra step to complete to ensure that the new name takes effect throughout the system.

1. Select **Administration > Object Text**.
2. Expand the folders for the Object type of the filter that you renamed.
3. Expand the **Filters** folder.
4. Expand the filter that you renamed.
5. In the **Locale Code** column, select *en_US*.
6. In **Label** enter the new name of filter.
7. Click **Save**.
8. Repeat for other locale codes if needed.

Deleting filters (Standard UI)

When you delete a filter for an Object type, it is permanently deleted from the system and cannot be restored.

If the filter is associated with object views in a profile (such as a Filtered List View, Grid View, or table on the My Work tab of a Home page), the filter, when deleted, is immediately removed from the view and is no longer available to users who are assigned that profile.

Procedure

1. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. Click the name of the object type to modify.

3. On the **Filters** tab, select the filters you want to delete.
4. Click **Delete**.

Dependent field behavior

You can configure a field so that its behavior - Visible, Editable, or Required - is dependent upon some value selected by a user in another field or set of fields.

A dependent field can have multiple behaviors and controlling fields. When you add a dependent field, configure the field and a behavior. Then, select the field and value that control the behavior.

If you want a dependent field to have multiple behaviors, such as Required and Visible, configure the field separately for each behavior.



Attention: If you configure a field to be required, it is still required even if it is not visible. This ability is for cases where the hidden field is updated by a separate activity, but the field is still required.

If you have multiple controlling fields for a specific behavior, you configure what conditions must be met before the behavior of the dependent field is triggered. The conditions are identified in the following list:

- Dependent fields cannot include System Fields.
- Dependent field behavior is not supported for custom forms.
- Controller fields must be enumerated string lists (single or multi-selectable) or Actor fields (User Selector, Group Selector, User/Group Selector, Multi User Selector, Multi Group Selector, or Multi User/Group Selector). If you configure a controller field with multiple values that are combined with an AND, all controller values or criteria must match. If you configure a controller field with multiple values that are combined with an OR, only one of the controller values or criteria must match. When the values or criteria match, the dependent field behavior is triggered.
- Computed fields and report fragment fields can have only a behavior of Visible.

Field dependencies can be defined in either the Task Focused UI or the Standard UI. In the Task Focused UI, functionality is centralized from the  > **Solution Configuration** > **Objects** task.

Important: If a field level security rule is applied to the controlling field, field dependencies that use the controlling field can no longer function as expected. The security restrictions that are built into the field level security rule apply to actions throughout the system and, therefore, prevent the field dependency from being evaluated. This behavior is true in views in both the Standard UI and the Task Focused UI. For more information, see [“Field level security” on page 133](#).

In the Task Focused UI:

- Dependent field behaviour is applied in Grid Views, Task Views, Creation Views, and Quick Views.
- In Grid Views, if a dependent field column is shown, the column values adhere to the field dependency behavior.

In the Standard UI:

- Dependent fields can be applied to Filtered List Views, Context Views, Grid Views, and Detail Views. They cannot be applied to Folder Views, List Views or Home Page Filters.
- On the Filtered List View page, if a dependent field column is shown, the column values adhere to the field dependency behavior.
- When users edit an object in Detail View, fields that are hidden due to how the field dependencies are configured can display as empty space.

Example

You want to know who performs a control activity if a user selects No to the question **Does the Control Owner perform the Control?**

You could configure the behavior of the field **Does the Control Owner perform the Control?** to be dynamic so that the field is both visible and required only if the user selects No to the question **Does the Control Owner perform the Control?**. If the user selects Yes, then this field would remain hidden from the user.

The **Does the Control Owner perform the Control?** field is considered the *dependent* field as the behaviors of this field (Required and Visible) depend on the value (No) selected in the *controller* field, **Does the Control Owner perform the Control?**.

Adding and working with dependent fields (Task Focused UI)

The dynamic behavior of dependent fields can be used to help guide users during the creation or editing of an object.

Before you begin

Log on with a user that has the Object Types application permission.

About this task

For more information about dependent fields, see [“Dependent field behavior” on page 278](#).

Field dependencies can be enabled, disabled, copied and deleted.

When a dependent field is disabled, the application does not enforce the conditions that control the behavior of the dependent field.

If you have multiple field dependencies that use the same controller conditions, click **Copy Controllers to New** to quickly duplicate existing controller conditions to the same or different dependent fields within the same object type.

When deleting field dependencies, if a dependent field is also used as a controller in other dependencies, you must first remove the dependencies on that field before deleting it. If you want to keep a dependent field but do not want its behavior, you can disable it rather than deleting it.

If you create field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".

Note that if an administrative user creates field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Click an object type.
3. Expand the **Field Dependencies** section.
4. Click **New Dependency**.
5. From the **Dependent Field**, select a field from the list.
6. In **Behavior Type**, select one of the following values:

Table 111. Behavior Type values	
Value	Description
Required	Require the user to enter a value in the dependent field only if the controlling field is selected.  Attention: If you configure a field as required, it is required even if it is not visible. This ability is for cases where the hidden field is updated by a separate activity, but the field is still required.
Editable	Enable the user to modify this dependent field only if the controlling field is selected. Otherwise, the dependent field is read only.
Visible	Display the dependent field to the user only if the controlling field is selected. Otherwise, the dependent field are hidden from view.

7. Select a value in **Controlling Field Logic**:

Table 112. Controlling Field Logic	
Select this value	If you want
And	All the selected controller fields to be used to meet the condition. This is the default operator value.
Or	Only one of the selected controllers to be used to meet the condition.

8. Click **Add** in **Controlling Fields**.

- Choose a field in **Controlling Field**.
- In the **Controlling Values** box, select one or more values from the list and click **Add**.
- Set **End User** to true or false, if displayed. It compares the field to the signed on user.
- Click **Create**.
- Add more controlling fields, as needed.

9. Click **Create**.

The newly created field dependency is listed on the **Field Dependencies** pane.

Adding dependent fields (Standard UI)

The dynamic behavior of dependent fields can be used to help guide users during the creation or editing of an object.

About this task

For more information about dependent fields, see [“Dependent field behavior” on page 278](#).

OpenPages with Watson supports standard multi-select functionality on the detail page.

Note that if an administrative user creates field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".

Procedure

- With the Object Types application permission set, select **Administration > Object Types**.

2. Click the name of the object type to modify.
3. On the **Field Dependencies** pane, click **Add**.
4. From the **Select Dependent Field**, select a field from the list.
5. In **Dependent Field Behavior**, select one of the following values:

Table 113. Dependent Field Behavior values	
Value	Description
Required	Require the user to enter a value in the dependent field only if the controlling field is selected.  Attention: If you configure a field as required, it is required even if it is not visible. This ability is for cases where the hidden field is updated by a separate activity, but the field is still required.
Editable	Enable the user to modify this dependent field only if the controlling field is selected. Otherwise, the dependent field is read only.
Visible	Display the dependent field to the user only if the controlling field is selected. Otherwise, the dependent field are hidden from view.

6. Click **Next**.
7. On the **Select Controller(s)** page, click the **Controlling Field** and choose a field from the list.
8. In the **Controlling Values** box, select one or more values from the list and click **Add**.
9. If you have multiple controller fields, click **Operator** and choose one of the following logical operator values:

Table 114. Logical operator values	
Select this value	If you want
And	All the selected controller fields to be used to meet the condition. This is the default operator value.
Or	Only one of the selected controllers to be used to meet the condition.

10. Click **Finish**.
11. To create additional dependent fields, complete one of the following tasks:

Table 115. Create additional dependent fields		
If you want to	And the Controllers are	Then
Add another behavior to the same dependent field - OR - Create another dependent field	the same as those selected in Step 4	Complete one of the following steps: • Copy the controller conditions to the new dependent field (see “Copying controller conditions (Standard UI)” on page 282) • Repeat Steps 3 and 4

Table 115. Create additional dependent fields (continued)		
If you want to	And the Controllers are	Then
Add another behavior to the same dependent field - OR - Create another (different) dependent field	different from those selected in Step 4	Repeat Steps 3 and 4

The newly created dependent fields are listed on the **Field Dependencies** pane.

Copying controller conditions (Standard UI)

If you have multiple field dependencies that use the same controller conditions, you can use the "Copy Controllers to" function to quickly duplicate existing controller conditions to the same or different dependent fields within the same object type.

This method will save you time as it is generally faster and easier than individually adding multiple dependent fields that all have the same controller fields.

Procedure

1. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. Click the name of the object type to modify.
3. On the **Field Dependencies** tab:
 - a) Select the check box next to the controller field you want to copy.
 - b) Click the **Copy Controllers to** icon.
4. In the Dependent Field pane of the controller (or controllers) you want to copy, select one or more behaviors for each dependent field.
5. Click **Create**.

The newly created dependent fields with the copied controllers are listed on the Field Dependencies pane.

Modifying controllers for a dependent field (Standard UI)

After you create a dependent field, you can add, remove, or modify the fields that control the behavior of the dependent field.

About this task

In the case of multiple controllers, you can also change the operator that determines whether one or all the controller conditions must be met before the dependent field behavior is triggered.

Note that if an administrative user creates field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".

Procedure

1. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. Click the name of the object type to modify.
3. On the **Field Dependencies** pane:
 - a) Select the dependent field you want to modify.
 - b) Click **Edit**.
4. To modify the values of an existing controller field:
 - a) Click **Edit** under the **Actions** column.
 - b) In the **Edit Controller** box, modify the selected values as necessary.
 - c) Click **Save**.
5. To add another controller:
 - a) In the **Add Controller** pane, click the **Controlling Field** arrow and select a field from the list.
 - b) In the **Controlling Values** box, select one or more values from the list.
 - c) Click **Add**.
6. To remove a controller:
 - a) Select the check box next to the controller field you want to remove.

Note: To select all the controllers for removal, select the check box next to the Controlling Field column heading.
 - b) Click **Delete**.
7. To change the operator when there are multiple controllers, click the **Operator** arrow and select a value from the list.
8. Click **Save**.

Enabling and disabling field dependency behavior (Standard UI)

Dependent fields can be enabled or disabled. By default, dependent fields are enabled when created.

When a dependent field is disabled, the following occurs:

- The dependent field remains in the list on the **Field Dependencies** tab, and the value in the **Enabled** column changes from true to false.
- The application does not enforce the conditions that control the behavior of the dependent field.

If you select multiple dependent fields to enable or disable, the application switches the values accordingly. For example, if you select two dependent fields - the first field is enabled with a value of true and the second field is disabled with a value of false - the value of the first dependent field would switch to false making it disabled, and the second would switch to true making it enabled.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
2. From the list, click the name of the object type you want to modify.
3. On the **Field Dependencies** tab:
 - a) Select the check box next to the dependent field you want to enable or disable. You can select multiple boxes.
 - b) Click **Enable/Disable**.

The value in the **Enabled** column on the **Field Dependencies** tab for the selected dependent field changes as follows:

- If disabled, the value changes from true to false
- If enabled, the value changes from false to true

Deleting dependent fields (Standard UI)

You can delete a dependent field.

When you delete a dependent field, it is permanently removed from the list on the **Field Dependencies** tab, and all corresponding records for the dependency are deleted and cannot be restored.

Important: If a dependent field is also used as a controller in other dependencies, you must first remove the dependencies on that field before deleting it.

If you want to keep a dependent field but do not want its behavior, you can disable it instead. For details, see [“Enabling and disabling field dependency behavior \(Standard UI\)” on page 283](#).

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
2. From the list, click the name of the object type you want to modify.
3. On the **Field Dependencies** tab:
 - a) Select the check box next to the dependent field you want to delete. You can select multiple boxes.
 - b) Click **Delete**.

Results

The selected dependent field is removed from the list on the **Field Dependencies** tab.

Configuration settings for the Add New wizard

The Add New wizard provides a way for users to easily add new object instances from virtually anywhere in the system. The appearance and function of the wizard is configurable. Some of the configuration settings apply globally and some are profile and object type specific.

With the Add New wizard, users can create and save object instances from wherever they are in the system by entering only the minimum and most important information. There are several launch points for the wizard, depending upon user permissions:

- A global **Add New** icon appears on every page. It can be used to create any object type.
- An **Add New** icon appears in the toolbar for the Filtered List View, Grid View, or Home Page Filtered List View. It can be used to create an object instance that is of the same type as the object type of the list.
- An **Add New** option is available from a context menu when you right-click on a row in Filtered List View, Grid View, or a Home Page Filtered List. It can be used to create an object instance that is of the same type as the object type of the list, or any of the direct children of the object type in the row.
- An **Add New** option is available from the **Actions** menu in Detail and Activity Views. The option allows adding an instance of a specific object type.

In most instances, the Add New wizard provides the most convenient and efficient way to add object instances. However, the original add behavior is available in the following places in the program:

- From the Folder View
- From the **Add New** icon available from the Business Entity Object List View if the Folder View and Filtered List View are both disabled for Business Entity.
- From the **Add New** icon available from **My OpenPages > Project > Milestones**.
- From the **Add File** link available from **My OpenPages > Attachments > Browse**.

The Add New wizard consists of a series of tabs that users can move between by clicking the **Previous** and **Next** icons or by clicking the tabs. The tabs that are available to users are determined by the object type, the user's profile, and the configuration.

Create tab

The Create tab allows users to select an existing object from which to prepopulate the field values for the new object they are creating. Type a term in the **Search** field to find an exact match to the object name or description. Configuration determines the following behaviors:

- If this is not possible to create an instance for the specified object type, the tab will not appear
- If it is mandatory to create an object instance from an existing instance, the tab will appear and an object must be selected from the specified location before the user can move to another tab.
- If this creating an object instance from an existing instance is optional, the tab will appear and the user can either select an object from which to prepopulate field values or choose to create the new object from scratch by filling in all the field values manually.

For more information see, [“Controlling the ability to use a template object when using the Add New wizard” on page 287](#)

Parents tab

The Parents tab allows users to identify the primary parent; the one in whose context the new object will be created. For most configurations, selecting a primary parent is required. This tab also allows users to select additional secondary parents of the same or different object type as the primary parent. Type a term in the **Search** field to find an exact match to the object name or description.

Object-specific tabs

One or more fields tabs follow the Parents tab. They contain the fields available to users for the specified object type. The tabs and fields displayed are driven by the view definition used for the Add New wizard.

The view definition comes from an Activity View named **Add New** for this object type for the users' profile. The Activity View must have this name but its label can be different. For more information see, [“Creating Activity Views” on page 337](#).

The view definition comes from a Creation View named **Add New** for this object type for the users' profile. The Creation View must have this name but its label can be different. For more information see, [“Creation views” on page 327](#).

The following factors determine the view:

- If the Activity View is not present and enabled, then the Detail View is used.
- If the Detail View is not enabled, then the default Object View is used
- Sections in the view definition become tabs in the Add New wizard. Fields are presented in the same sections and in the same sequence in the Add New wizard as they are in the view definition. If there are fields before the first defined section, or if there are no sections in the view definition, then a tab labeled **Properties** is created to hold those fields. Read-only settings in the view definition are respected by the Add New wizard.
- Certain fields and field types are not supported in the Add New wizard. The following fields are not included in the Add New wizard if you configure them in the view definition:
 - System audit trail fields: Create By, Last Modified By, Created Date, Last Modified Date
 - System location field: Folder
 - System derived fields: Orphan, Business Entity Hierarchy, Primary Association Path
 - Computed fields
 - Reporting fragments

Associated children tabs

If there are child objects that can be linked to the object instance, one or more association tabs may follow the object-specific tabs.

For example, if you are creating a questionnaire assessment, you can choose the processes or assets to associate with the questionnaire assessment.

Type a term in the **Search** field to find an exact match to the object name or description.

Review tab

The Review tab displays all of the information from the preceding tabs in read-only mode. It provides users with an ability to perform a review of their choices and entries before they save their work.

Tab labels are displayed in the wizard with a circle beside each tab label. When a circle is white, it means that all of the required fields for that tab are either not complete or have failed validation. When all required fields in a tab are complete and all field values have passed validation, the circle for that tab is green. An object instance will not be created until the circles for all the tabs are green.

The Add New wizard supports existing configuration parameters, including Save as Draft, Auto-naming, Dependent Fields, and Dependent Picklists.

The Save As Draft feature can be configured to display a **Save As Draft** icon when a user creates a new object instance. This means that users can save object data without completing all the required fields. The **Save As Draft** icon is displayed next to the **Save** icon in the Add New wizard. For information on how to specify the Save as Draft settings, see [“Configure the ability to create a draft copy of an Object \(Standard UI\)” on page 260](#)

For most object types, you can auto-generate their names when they are created. This allows users to enforce internal naming policies and ensure unique object names. You can turn auto-naming on or off for each object type individually. For information on how to specify the Auto-naming feature, see [“Object auto-naming settings” on page 609](#).

You can configure a field so that its behavior (Visible, Editable, or Required) is dependent upon some value selected by a user in another field or set of fields. For more information see, [“Dependent field behavior” on page 278](#)

You can configure a list of items (drop-down or list box) so that the items in the list are filtered based upon some value selected by a user in another list. For more information see, [“Configuring dependent picklists” on page 288](#)

Controlling the availability of object types in the Add New wizard

You can configure which object types cannot be created from the Add New wizard with a setting that takes effect for all users and all profiles.

Procedure

1. From the menu bar, click **Administration > Settings**.
2. Click **Applications > GRCM > Add New Wizard**.
3. Click **Object Types Disabled**.
4. In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (.). Be sure to use the object names and not the object labels.
5. Click **Save**.

Controlling the display of tabs with no fields in the Add New wizard

You configure whether fields tabs without any fields to display appear in the Add New wizard as disabled or do not appear at all. The Add New wizard will dynamically hide or show or enable field tabs as they become empty or not empty as a result of field dependencies.

Procedure

1. From the menu bar, click **Administration > Settings**.
2. Click **Applications > GRCM > Add New Wizard**.
3. Click **Show Empty Sections**.

4. In the **Value** box, type false if you do not want to show empty sections and tabs. Type true if you want empty sections to appear but be disabled.
5. Click **Save**.

Controlling the ability to use a template object when using the Add New wizard

You can specify whether users must create new object instances from an existing object instance, whether they can optionally create new object instances from an existing object instance, or whether the user should create the object from scratch.

About this task

If you want users to be able to create object instances either from scratch or from an existing object instance, ensure that the object type name does not appear in either the **Cannot Create from Existing** setting or in the **Must Create from Existing** setting.

If you do not want users to create object instances from an existing object instance, include the object type names in the **Cannot Create from Existing** setting.

If you want to force users to create object instances from an existing object instance, include the object type names in the **Must Create from Existing** setting.

The **Cannot Create from Existing** and the **Must Create from Existing** settings can be configured globally for all profiles, can be configured individually for each profile, or in combination:

- To configure globally for all profiles, enter the desired information in the **All Profiles** setting under the **Cannot Create from Existing** and the **Must Create from Existing** folders.
- To configure individually for each profile, create a setting for each profile, whose name is the name of the profile, under the **Cannot Create from Existing** and the **Must Create from Existing** folders. Enter the desired information in each profile setting.
- To configure a combination of globally but to override that configuration for specific profiles, create a setting for each profile you wish to override, whose name is the name of the profile, under the **Cannot Create from Existing** and the **Must Create from Existing** folders. Enter the desired information in each of the specific profile settings. Enter the value you desire for all other profiles in the **All Profiles** setting.

Procedure

1. From the menu bar, click **Administration > Settings**.
2. Click **Applications > GRCM > Add New Wizard**.
3. To enter information that applies to all profiles:
 - a) Expand the **Cannot Create from Existing** or the **Must Create from Existing** folder.
 - b) Select the **All Profiles** setting and enter the desired information.
4. To enter information for a specific profile, you must first create a setting for that profile under the **Cannot Create from Existing** or the **Must Create from Existing** folder, which has the exact name of the profile. For more information, see [“Custom settings” on page 633](#)
5. For **Cannot Create from Existing** settings, enter a comma separated list of object type names, not labels, and click **Save**.
6. For **Must Create from Existing** settings, enter a line for each object type where the format is multiple lines separated by carriage return - line feed, each formatted as <object system name><colon><starting path>, and click **Save**. The existing object instances to be used as templates must be located under the starting path specified.

Controlling the default object type in the parent picker in the Add New wizard

You can specify the default object type in the parent picker. For each desired object type, you can specify a series of parent object type defaults; the first type available to this user will be set as the default.

About this task

You can configure globally, for individual profiles, or both:

- To configure globally for all profiles, enter the desired information in the **All Profiles** setting under the **Parent Object Type Preferences** folder.
- To configure individually for each profile, create a setting for each profile, whose name is the name of the profile, under the **Cannot Create from Existing** and the **Must Create from Existing** folders. Enter the desired information in each profile setting.
- To configure a combination of globally but to override that configuration for specific profiles, create a setting for each profile you wish to override, whose name is the name of the profile, under the **Parent Object Type Preferences** folder. Enter the desired information in each of the specific profile settings. Enter the value you desire for all other profiles in the **All Profiles** setting.

It is not necessary to specify this information; the system will choose defaults for any object type or profile not specified.

Procedure

1. From the menu bar, click **Administration > Settings**.
2. Click **Applications > GRCM > Add New Wizard > Parent Object Type Preferences**.
3. To enter information that applies to all profiles select the **All Profiles** setting and enter the desired information.
4. To enter information for a specific profile, you must first create a setting for that profile under the **Parent Object Type Preferences** folder, which has the exact name of the profile. For more information, see [“Custom settings” on page 633](#)
5. For each object type in the setting, specify the default parent object type to be selected in the Select Parents Narrow By panel. Format is multiple lines separated by carriage return - line feed, each formatted as <object type to be created system name><colon><highest priority object type system name to be parent><comma><second highest priority object type system name to be parent>, and so on, as shown in the following example:

Resource:SOXBusEntity,RiskSubEntity

ReviewComment:AuditProgram,Finding,Workpaper

RiskAssessment:SOXBusEntity

Configuring dependent picklists

You can configure a list of items so that the items in the list are filtered based upon some value selected by a user in another list.

The filtering of lists can be used to help guide users in the selection of relevant values from lists during the creation or editing of an object.

Dependent picklists can be defined in either the Task Focused UI or the Standard UI. In the Task Focused UI, functionality is centralized from the  > **Solution Configuration > Objects** task.

Example

Both the Risk Category and Risk Subcategory fields of a Risk object (SOXRisk) have many items in their respective lists from which a user can choose, and you want only the values of "Theft and Fraud" and "Security Systems" to be displayed in the Risk Subcategory list when a user selects "External Fraud" from the Risk Category list.

To filter the list, you would map the Risk Subcategory values of "Theft and Fraud" and "Security Systems" to the Risk Category value of "External Fraud".

The Risk Subcategory field with its selected values is considered the *dependent picklist* as the behavior of this list depends upon the value selected in the Risk Category field or *controller picklist*.

Adding and working with dependent picklists (Task Focused UI)

When you create a dependent picklist, you map one or more dependent field list values to one or more controlling field list values.

Before you begin

Log on with a user that has the Object Types application permission.

About this task

For more information about dependent picklists, see [“Configuring dependent picklists” on page 288](#).

Dependent picklists can be enabled, disabled, and deleted.

When a dependent picklist is disabled, the application does not enforce the conditions of the picklist.

If you want to keep a dependent picklist but do not want to enforce it, you can disable it rather than deleting it.

If you create field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".



Attention: When using the bulk update feature, the dependent picklists do not change values when the controlling value changes. Instead, all values from both the controller and the dependent picklist are displayed. Validation of selected values is done before the objects are saved and conflicts are reported back to the user.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Click an object type.
3. Expand the **Dependent Picklists** section.
4. Click **New Dependency**.
5. From the **Dependent Field**, select a field from the list.
6. Click **Add** in **Controlling Fields**.
 - a) Choose a field in **Controlling Field**.
 - b) Under **Controller values**, expand a value.
 - c) Click **Add** next to **Dependent Values**.
 - d) Select the values that you want to map.
 - e) Click **Create**.
 - f) Map more values, as needed.
7. Click **Create**.

The newly created dependent list is listed on the **Dependent Picklists** section.

Example

The following example shows how Risk Category, the *controlling field*, and Risk Subcategory, the *dependent field*, are mapped on Risk object (SOXRisk) type.

Each controller value group contains values in the controlling picklist (Risk Category in this example) that are mapped to values in the dependent picklist (Risk Subcategory in this example).

The Risk Subcategory values "Theft and Fraud" and "Unauthorised Activity" are selected for Internal Fraud. "Theft and Fraud" and "System Security" are selected for External Fraud. If a user selects "Internal Fraud" as the Risk Category, only "Theft and Fraud" and "Unauthorised Activity" values will be displayed on the Risk Subcategory list. Similarly, if a user selects "External Fraud" as the Risk Category, only the "Theft and Fraud" and "Systems Security" values will be displayed in the Risk Subcategory list.

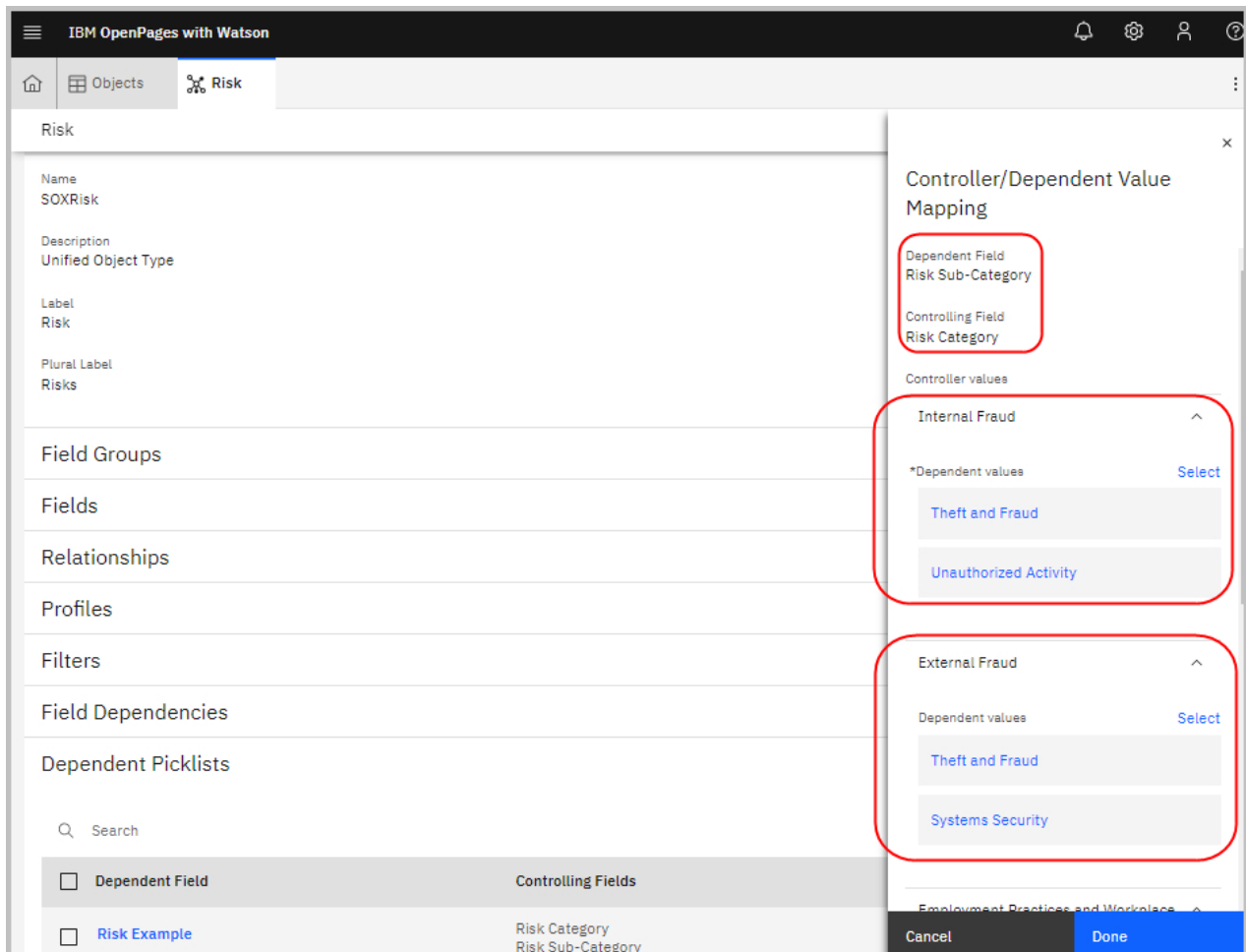


Figure 16. Sample picklist mapping

Adding dependent picklists (Standard UI)

When you create a dependent picklist, you map one or more dependent field list values to one or more controlling field list values.

About this task

Note that dependent picklist behavior is not supported for custom forms.

Note that if an administrative user creates field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result

in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".



Attention: When using the bulk update feature, the dependent picklists do not change values when the controlling value changes. Instead, all values from both the controller and the dependent picklist are displayed. Validation of selected values will be done before the objects are saved and any conflicts are reported back to the user.

Figure 17 on page 291 shows a partial Picklist Mapping grid for the "Category" and "Subcategory" drop-down lists - both are Risk object (SOXRisk) type fields.

Each column represents a value in the controlling picklist ("Category" in this example), and each row represents a value in the dependent picklist ("Subcategory" in this example).

In Figure 17 on page 291, the "Subcategory" values of "Unauthorised Activity" and "Theft and Fraud" are selected for the "Internal Fraud" value, and "Theft and Fraud" and "System Security" are selected for the "External Fraud" value. If a user selects "Internal Fraud" as the category, only the "Unauthorised Activity" and "Theft and Fraud" values will be displayed on the Subcategory list. Similarly, if a user selects "External Fraud" as the "Category", only the "Theft and Fraud" and "Systems Security" values will be displayed on the Subcategory list.

Object Types: SOXRisk		
Selected Dependent Picklist "Subcategory" and Controlling Picklist "Category"		
Picklist Mapping		
Category:	Internal Fraud	External Fraud
Subcategory:	Unauthorised Activity Theft and Fraud Systems Security Employee Relations	Unauthorised Activity Theft and Fraud Systems Security Employee Relations

Figure 17. Sample picklist mapping grid

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
2. From the list, click the name of the object type you want to modify.
3. On the **Dependent Picklists** tab, click **Add**.
4. On the **Add Dependent Picklist** page:
 - a) Click the **Select Controlling Picklist** arrow and choose a controlling field from the list.
 - b) Click the **Select Dependent Picklist** arrow and choose a dependent field from the list.
5. On the **Picklist Mapping** page, for each controlling value in a column heading for which you want to create a filtered list, select one or more dependent field values in the corresponding column row.

Note: To select or clear a value from a row, click the name of the value.

6. Click **Finish** to save your changes.

The newly created dependent picklists are listed on the **Dependent Picklists** tab.

Modifying picklist dependency behavior (Standard UI)

After you create a dependent picklist, you can modify the values that are displayed in the dependent picklist.

About this task

Note that if an administrative user creates field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
2. From the list, click the name of the object type you want to modify.
3. On the **Dependent Picklists** tab:
 - a) Select the check box next to the dependent picklist you want to modify.
 - b) Click **Edit**.
4. To modify the values that are displayed in a dependent picklist by a controlling value:
 - a) Navigate to the column heading with the controlling value.
 - b) Click a value in the column row to either select or clear a value.
5. Click **Save**.

Enabling and disabling picklist dependency (Standard UI)

Dependent picklists can be enabled or disabled. By default, dependent picklists are enabled when created.

When a dependent picklist is disabled, the following occurs:

- The dependent picklist remains in the list on the **Field Dependencies** tab, and the value in the **Enabled** column changes from true to false.
- The application does not enforce the conditions that control the behavior of the dependent picklist.

If you select multiple dependent picklists to enable or disable, the application switches the values accordingly. For example, if you select two dependent picklists - the first picklist is enabled with a value of true and the second picklist is disabled with a value of false - the value of the first dependent picklist would switch to false making it disabled, and the second would switch to true making it enabled.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
2. From the list, click the name of the object type you want to modify.
3. On the **Dependent Picklists** tab:
 - a) Select the check box next to the dependent picklist you want to enable or disable.
 - b) Click **Enable/Disable**.

The value in the **Enabled** column on the **Dependent Picklists** table changes as follows for the selected dependent picklist:

- If disabled, the value changes from true to false
- If enabled, the value changes from false to true

Deleting a dependent picklist (Standard UI)

You can delete a dependent picklist.

When you delete a dependent picklist, it is permanently removed from the list on the **Dependent Picklists** tab and cannot be restored.

Note: If you want to keep a dependent picklist but do not want its behavior, you can disable it instead. For details, see [“Enabling and disabling picklist dependency \(Standard UI\)”](#) on page 292.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
2. From the list, click the name of the object type you want to modify.
3. On the **Dependent Picklists** tab:
 - a) Select the check box next to the dependent picklist you want to delete. You can select multiple boxes.
 - b) Click **Delete**.

Results

The selected dependent picklist is removed from the list on the **Dependent Picklists** tab.

Excluding fields from a subsystem

IBM OpenPages with Watson contains multiple subsystems or components that comprise a larger software system.

These subsystems (for example, Reporting Schema and Reporting Framework), typically use field definitions. In some situations, a field that is applicable to one subsystem may not be applicable to another.

For example, suppose that you want to streamline the number of fields that are used for generating Test (SOXTest) object reports. You are not required, for example, to produce a report on Testing Steps, a field that is part of the Test object. You could exclude the Testing Steps field from the Reporting Schema and the Reporting Framework subsystems. When you regenerate the reporting schema and the framework, the Testing Steps field is ignored and is excluded from the schema and framework.

Selecting the fields to exclude

When you exclude a field from a subsystem, the subsystem ignores the excluded field.

The following table identifies that action that occurs when selected fields are excluded:

Table 116. Field exclusions and results

Fields excluded from this subsystem	Results
Reporting Schema	Any application components that use the field need to be updated to remove references to the excluded field. For example, you might need to update security rules, reports, and filtered list views. If you exclude a field from the reporting schema, also exclude it from the reporting framework. If you use global search, also remove the field from global search. For more information, see “Enabling or disabling object types or fields for global search” on page 655. Note: A field that is excluded from the reporting schema must also be excluded from global search. If you want to use global search on a field, do not exclude it from the reporting schema. Note: When you use the IBM OpenPages REST API, a select * statement returns all fields except the fields that are excluded from the reporting schema. For more information, see the <i>IBM OpenPages with Watson GRC REST API Guide</i>.
Reporting Framework	Any reports (existing or future) that reference these fields fail unless the excluded field is also removed from the report.

Procedure

1. With the Object Types application permission set, select **Administration** and click **Object Types**.
2. From the list, click the name of the object type to modify.
3. On the **Field Exclusions** pane for object type, click **Exclude**.
4. Complete the following steps on the **Exclude Fields** page:
 - a) In the **Select Field** field, select the fields that you want to exclude from the subsystem.
 - b) In the **Select Subsystem** field, select the subsystem.
5. Click **Exclude**.
The newly excluded fields are listed on the **Field Exclusions** tab.
6. To exclude fields from a different object type, repeat Steps 1 - 5.
7. If you excluded fields from the Reporting Schema subsystem, re-create the reporting schema.
For more information, see [“Creating or recreating the reporting schema \(Standard UI\)”](#) on page 163.
8. If you excluded fields from the Reporting Schema or from the Reporting Framework subsystem, regenerate the reporting framework.
For more information, see [“Updating the reporting framework \(Standard UI\)”](#) on page 978.

Changing the subsystem for an excluded field

You can change the subsystem for individual fields that have been excluded from a subsystem.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
2. Select the name of the object type you want to modify.
3. On the **Field Exclusions** tab:
 - a) Select the check box next to the excluded field you want to modify.

- b) Click **Edit**.
- 4. In the **Select Subsystem** box, modify the subsystem.
- 5. Click **Save**.
- 6. If you modified the list of fields that are excluded from the Reporting Schema subsystem, re-create the reporting schema.
For more information, see [“Creating or recreating the reporting schema \(Standard UI\)” on page 163](#).
You must re-create the reporting schema for the changes to take effect.
- 7. If you modified the list of fields that are excluded from the Reporting Schema or from the Reporting Framework subsystem, update the reporting framework.
For more information, see [“Updating the reporting framework \(Standard UI\)” on page 978](#).

Removing excluded fields

You can remove a field from the list of excluded fields.

When you remove a field from the list of excluded fields, the field is removed from the **Field Exclusions** list for the object type.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
2. From the list, click the name of the object type you want to modify.
3. On the **Field Exclusions** tab:
 - a) Select the check box next to the excluded field you want to remove. You can select multiple boxes.
 - b) Click **Remove**.
 - c) If prompted, click **OK**.

The selected excluded field is removed from the **Field Exclusions** list for the object type.
4. If you modified the list of fields that are excluded from the Reporting Schema subsystem, re-create the reporting schema.
For more information, see [“Creating or recreating the reporting schema \(Standard UI\)” on page 163](#).
You must re-create the reporting schema for the changes to take effect.
5. If you modified the list of fields that are excluded from the Reporting Schema or from the Reporting Framework subsystem, update the reporting framework.
For more information, see [“Updating the reporting framework \(Standard UI\)” on page 978](#).

Chapter 11. Profiles

Profiles provide end users with a localized view of information that is directly related to their responsibilities.

Use profiles to configure objects, custom forms, fields, and object views. When you change a setting in a profile, the change is dynamic and the change is immediate. In the Task Focused UI, reports can be added to profiles.

Each user has one or more profiles available to them for their logon session.

You can use profiles to restrict the object types that individual users can view. You can also define the fields in each object that are visible to them. If an object type is absent from a profile, that object type is hidden from users of that profile. You can also assign reports to a profile.

Create profiles by cloning them from existing profiles, then modifying the new profile. A standard profile, called Default, is provided. You can use it as a template to create other profiles. The profiles that you create and assign to users are standalone. No inheritance occurs from one profile to another profile, including the Default profile.

When you associate a profile to a group, all users in the group have that profile added to their Allowed Profiles list. The profile is stored with the user, not the group. If a user is later added to the group, they will not be assigned the profile that was earlier assigned to the users of the group.

You can also designate any profile as the default profile or fallback profile. For more information, see [“Setting a default or fallback profile” on page 300](#).

Important:

- If you assign a user to a different profile, the change becomes effective immediately with no action required on the part of the user. While a user is logged in, you can assign different profiles to the user but you should not change their "Current Profile" or remove it from the list of "Allowed Profiles" because that may result in the user losing unsaved work.
- Users can change from one assigned profile to another themselves. For more information, see "Changing your profile" in the *IBM OpenPages with Watson User Guide*.

You can associate available objects with any profile and disassociate them later. However, each profile contains a group of required objects that you cannot disassociate from the profile. The following table lists these required object types:

Table 117. Required object types	
Object Type	Label
SOXBusEntity	Business Entity
SOXSignature	Signature
SOXExternalDocument	Link (this is an external URL link)

Guidelines for working with profiles

Following are some suggested guidelines for working with profiles.

- Create and enable a default profile and a fallback profile before you create any other profiles for users and groups. For more information, see [“Setting a default or fallback profile” on page 300](#).
- Consider designating the most commonly used profile as the default profile.
- Do not disable, delete, or disassociate profiles that users are actively using because it may disrupt their work. In particular, do not do so unless you have created and enabled a fallback profile that users with no other active profile can use to log on.

- Associate one or more new profiles to a user or group before disabling or deleting all of their existing ones.

Accessing profiles

From a profile, you can modify profile information and associate users and groups.

Before you begin

Log on to IBM OpenPages with Watson as a user with the Profiles application permission set. For more information, see [“Types of application permissions” on page 91](#).

About this task

Profiles can be managed using tasks in either the Task Focused UI or the Standard UI. Changes made in one interface are immediately reflected in the other. Functionality between the two user interfaces is mostly the same except that in the Standard UI you can configure views for the Standard UI and change the display order of fields for a selected object type.

Additionally, in the Task Focused UI, the Display Type attribute is defined directly on fields. In the Standard UI, the Display Type attribute is defined on profiles.

Procedure

Click  > **Solution Configuration** > **Profiles**.

Or, in the Standard UI, click **Administration** > **Profiles**.

Creating a profile (Task Focused UI)

You can create a new profile based on an existing profile, including the "Default" profile that is supplied with the product.

Procedure

1. Click  > **Solution Configuration** > **Profiles**.

Or, in the Standard UI, click **Administration** > **Profiles**.

2. Click **New Profile**.
3. Enter a **Name** for the profile. The name should be easily recognizable by users and identify the purpose for which it is designed. Profile names cannot be translated or changed after they are created.
4. Enter a **Description**.
5. Click **Based on Profile** and select a profile to use as a template for the new profile.
6. If you want the new profile to be the default profile, select **Default**. For more information, see [“Setting a default or fallback profile” on page 300](#).
- Important:** Creating a default profile might affect the way IBM OpenPages with Watson handles objects and profiles.
7. If you want the new profile to be the fallback profile, select **Fallback**. For more information, see [“Setting a default or fallback profile” on page 300](#).
8. Select **Enabled**.
9. Click **Done**.

The profile is created and added to the list of profiles.

10. Click the name of the profile and finish configuring the profile by completing following tasks:

Table 118. Profile configuration tasks	
To ...	See this topic ...
associate and disassociate users and groups	“Associating users and groups to a profile” on page 302 “Disassociating users and groups from a profile” on page 304
include and exclude object types	“Including object types in a profile” on page 304 “Removing object types from a profile” on page 305
associate reports	“Adding reports to a profile” on page 305

Creating a profile (Standard UI)

You can create a new profile based on an existing profile, including the "Default" profile that is supplied with the product.

Procedure

1. Select the **Administration** menu and click **Profiles**.
2. On the **Profiles** table, click **Add**.
3. On the **Add Profile** page, type a name for the profile. The name should be easily recognizable by users and identify the purpose for which it is designed. Profile names cannot be translated or changed after they are created.
4. Click **Based on Profile** and select the profile to use as a template for the new profile.
5. If you want the new profile to be the default profile, select **Default**. For more information, see [“Setting a default or fallback profile” on page 300](#)).

Important: Creating a default profile might affect the way IBM OpenPages with Watson handles objects and profiles.

6. If you want the new profile to be the fallback profile, select **Fallback**. For more information, see [“Setting a default or fallback profile” on page 300](#)).
7. Click **Create**.
8. To configure the profile, do one of the following tasks:

Table 119. Profile configuration tasks	
If you want to do this...	Then see this topic for details...
associate and disassociate users	“Associating users and groups to a profile” on page 302 “Disassociating users and groups from a profile” on page 304
include and exclude object types	“Including object types in a profile” on page 304 “Removing object types from a profile” on page 305
set up a Home page	“Home page” on page 309
configure views for an object type	“Configure views for objects” on page 322

This video demonstrates how to create profiles and add object types and views to a profile:

<https://youtu.be/-iiyrMWz3Oo>

Setting a default or fallback profile

You can set default and fallback profiles for users and groups.

Before you create a default or fallback profile, see [“Guidelines for working with profiles”](#) on page 297.

You can designate any profile as the default profile for a user or group. Any previously designated profile loses this default designation when you select another profile as the default profile. In an application upgrade, the default profile includes all the object properties of the previous version of the application. All profiles are standalone; there is no inheritance from the default profile.

When you create users and add profiles, the default profile serves as the profile that is used if no other profile is selected. You do not need to designate a default profile. If no profile is designated as the default profile, the fallback profile will be used.

The fallback profile allows a user who is either not associated with any profile, or whose profile is disabled or deleted, to log on to OpenPages with Watson. Only one profile can be designated as the fallback profile. If you choose to designate a profile as the fallback profile, the existing fallback profile (if there is one) loses this designation. The fallback profile is optional, however it's a best practice to designate and enable one so users without any other enabled profiles can log on.

Procedure

1. Click  > **Solution Configuration** > **Profiles**.

Or, in the Standard UI, click **Administration** > **Profiles**.

2. Click the name of a profile.

3. Click **Edit**.

4. On the **Edit Profile** page:

- a) Select one or more of the following options:

- **Default** - to make this profile the default profile

Tip: Consider designating the most commonly assigned profile as the default profile for users and groups.

- **Fallback** - to make this profile the fallback profile

- **Enabled** - to enable this profile (Task Focused UI only)

- b) Optionally, enter or change the description of the profile.

- c) Click **Done**.

Editing a profile

You can modify the description of a profile or designate the profile as the default profile or fallback profile.

Procedure

1. Click  > **Solution Configuration** > **Profiles**.

Or, in the Standard UI, click **Administration** > **Profiles**.

2. Click the name of a profile.

3. Click **Edit**.

4. Make your edits. Note that profile names cannot be translated or changed after they are created.

5. Click **Done**.

Deleting a profile

You can delete a profile.

Important: If you delete a profile, it immediately disappears from the system and you cannot retrieve it. It is immediately unavailable to currently logged in users or to users who subsequently log in. If you are not sure if you might need the profile again, disable it instead.

Before deleting a profile, see [“Guidelines for working with profiles” on page 297](#).

For users with multiple profiles, the current profile becomes the first profile in the alphabetical list of their allowed profiles. If you delete the only profile that is assigned to a user, the user can still log in using the fallback profile if one exists and is enabled. For more information, see [“Setting a default or fallback profile” on page 300](#)

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
Or, in the Standard UI, click **Administration** > **Profiles**.
2. Select the box next to each profile you want to delete.
3. Click **Delete**.
4. Click **Delete** to confirm the deletion (OK in the Standard UI).

Enabling a profile

When you enable a profile the status of the profile changes from Inactive to Active, and the profile immediately becomes available to users who are assigned that profile (either currently logged on users or to users who subsequently log on).

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
Or, in the Standard UI, click **Administration** > **Profiles**.
2. Click the name of a profile.
3. Click **Edit** (Task Focused UI only).
4. Click **Enable**.

The status changes to **Active**.

Alternatively, in the Task Focused UI, from the list of profiles, you can select the box next to one or more profiles and click **Enable**.

Disabling a profile

You can disable a profile.

Important: When you disable a profile, it is not deleted. It remains in the system, and the status of the profile changes from Active to Inactive. A disabled profile is immediately unavailable to users to currently logged in users or to users who subsequently log in.

Before disabling a profile, see [“Guidelines for working with profiles” on page 297](#).

For users with multiple profiles, the current profile becomes the first profile in the alphabetical list of their allowed profiles. If you disable the only profile that is assigned to a user, the user can still log in using the fallback profile if one exists and is enabled. For more information, see [“Setting a default or fallback profile” on page 300](#).

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
Or, in the Standard UI, click **Administration** > **Profiles**.
2. Click **Edit** (Task Focused UI only).
3. Click **Disable**.

The status changes to **Inactive**.

Alternatively, in the Task Focused UI, from the list of profiles, you can select the box next to one or more profiles and click **Disable**.

Associating profiles to a user

You can associate one or more profiles to a user or group. Having multiple profiles is beneficial for users that have more than one function and require a different profile for each one. It is also beneficial for administrators because it can reduce the number of profiles that they need to create and maintain.

Tip: It is more efficient to associate profiles to groups rather than individual users. Note that if a user is later added to the group, they will not be assigned the profile that was earlier assigned to the users of the group.

About this task

The following steps explain how to associate profiles from a user account. You can also associate profiles to users (and groups) from the profile page. For more information, see [“Associating users and groups to a profile” on page 302](#)

Note that from a group, it is not possible to assign a group to a profile. You must instead, go to the profile page and assign a group to the profile.

Procedure

1. Click  > **Users and Security** > **Users**.
Or, in the Standard UI, click **Administration** > **Users**.
2. Select the user that you want to assign a profile to.
3. In **Allowed Profiles**, select all the profiles that you want to assign to the user.
4. Optionally, you can change the user's current profile by selecting a different profile from the **Current Profile** list.

Warning: If you change a user's profile while they are logged on you might disrupt their work.

- If you remove the user's current profile from **Allowed Profiles**, the user's current profile is set to the first allowed profile in the alphabetical list.
- For existing users, the **Current Profile** is set to the user's current profile.
- For new users, the current profile is set to the default profile, if one exists and is enabled. If an enabled default does not exist, the current profile is set to the fallback profile, if one exists and is enabled. For more information, see [“Setting a default or fallback profile” on page 300](#).

5. Click **Save**. The changes take effect immediately.

Associating users and groups to a profile

You can associate users and groups to one or more profiles. Users that have no associated profiles use the fallback profile, if one exists.

For more information, see [“Setting a default or fallback profile” on page 300](#).

When you associate a profile with a user, the object types in that profile are available to that user. Additionally, you can select the fields within each object type that users of this profile can view.

When you associate a profile to a group, all users in the group have that profile added to their **Allowed Profiles** list. The profile is stored with the user, not the group. If a user is disassociated from a group, the profile is not disassociated from the user. Note that if a user is later added to the group, they will not be assigned the profile that was earlier assigned to the users of the group.

The profile that you associate with a user is not the current profile unless no current profile is selected.

Table 120. Associating users and groups to a profile	
If you select a...	Then this occurs...
user who has no profile	the currently selected profile is assigned to that user.
user who already has a profile assigned	the current profile stays the same, and the new profile is added to their list of allowed profiles.
group	all the members of that group are selected and each member is individually assigned the selected profile and listed on the Users section (Task Focused UI) or Associated Users tab (Standard UI).

About this task

The following steps explain how to associate users or groups to a profile on a profile page. You can also associate profiles from the user account. For more information, see [“Modifying user accounts” on page 86](#) and [“Associating profiles to a user” on page 302](#).

Procedure

1. Click  > **Solution Configuration > Profiles**.
Or, in the Standard UI, click **Administration > Profiles**.
2. Click the name of a profile.
3. In the Task Focused UI:
 - a) Go to the **Users** section.
 - b) Click **Add**.
 - c) Search for the user or group that you want to add.
 - d) Select it.
 - e) Click **Done**.
 - f) Repeat the steps for the next user or group.
4. In the Standard UI:
 - a) On the **Associated Users** table, click **Associate**.
 - b) In the **Associate users/groups with profile** box, select the users or user groups you want to associate with the profile. You can view individual users within a group by clicking the + box.
 - c) Click **Associate**.

This video for the Standard UI demonstrates how to configure multiple profiles for users, and how users can easily switch from one profile to another (Standard UI):

<https://youtu.be/amgQPw51Duo>

Disassociating users and groups from a profile

When you disassociate a user from a profile, that profile becomes immediately unavailable to that user.

If you disable or disassociate a user from their current profile, one of their available profiles becomes their current profile. If there are no other available profiles, the fallback profile is used. If no fallback profile is assigned, the user is unable to log on to the application. For more information, see [“Setting a default or fallback profile”](#) on page 300.

Before disassociating a profile, see [“Guidelines for working with profiles”](#) on page 297.

About this task

You can disassociate users from a profile. Alternatively, you can disassociate users from profiles from the user account. For more information, see [“Modifying user accounts”](#) on page 86.

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
Or, in the Standard UI, click **Administration** > **Profiles**.
2. Click the name of a profile.
3. In the Task Focused UI:
 - a) Go to the **Users** section.
 - b) Select the user or group with a check mark.
 - c) Click **Remove**.
 - d) Click **Remove** again to confirm.
4. In the Standard UI:
 - a) On the **Associated Users** table listing:
 - b) Select the box next to each user you want to disassociate from this profile.
 - c) Click **Disassociate**.
 - d) Click **OK**.

Including object types in a profile

When you include an object type in a profile, that object type is immediately visible to users who are assigned the selected profile. The object types that you select determine which menus appear and the contents of each menu.

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
Or, in the Standard UI, click **Administration** > **Profiles**.
2. Click the name of a profile.
3. In the Task Focused UI:
 - a) Go to the **Object Types** section.
 - b) Click **Add**.
 - c) Select the box next to each object type to add to the profile.
 - d) Click **Done**.
4. In the Standard UI:
 - a) On the **Object Types** table, click **Include**.

- b) On the **Available Object Types** page, select the box next to each object type you want to include in this profile.
 - c) Click **Include**.
5. To configure views for an object type, see [“Configure views for objects” on page 322](#) (Standard UI only).

Removing object types from a profile

When you remove (exclude) an object type from a profile, that object type is removed from the views in which it is used. It is no longer available to users who are assigned that profile.

Note: Certain object types are required. You get an error message if you try to remove them.

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
Or, in the Standard UI, click **Administration** > **Profiles**.
2. Click the name of a profile.
3. In the Task Focused UI:
 - a) Go to the **Object Types** section.
 - b) Select the box next to each object type that you want to remove from the profile.
 - c) Click **Remove**.
 - d) Click **Remove** again to confirm.
4. In the Standard UI:
 - a) From the **Object Types** table, select the box next to each object type that you want to exclude from the profile.
 - b) Click **Exclude**.
 - c) Click **OK** to remove the object type from view.

Results

The selected object type is removed from the list of object types for this profile. IBM OpenPages with Watson stores an excluded object, along with any associated data, in the repository. You can view it through reports.

Adding reports to a profile

When you add reports to a profile, users can add those reports to their Dashboard.

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
2. Click the name of a profile.
3. Go to the **Reports** section.
4. Click **Add**.
5. Select each report to add to the profile.
6. Click **Done**.

Results

The reports are added to the profile and enabled.

You can hide reports from dashboards by disabling the reports in the profile. Or, you can remove the report from the profile. Select the report and then click **Disable** or **Remove**.

Including fields in an object type

Including object fields for an object type in a profile makes those object fields available for selection within the various views.

The availability of a field for configuration within any view depends on whether or not that field is included or excluded in the object type for that profile. Including or excluding fields for object types in one profile does not affect object-type fields in other profiles.

Procedure

1. Click  > **Solution Configuration** > **Profiles**.

Or, in the Standard UI, click **Administration** > **Profiles**.

2. Click the name of a profile.

3. In the Task Focused UI:

- a) Go to the **Object Types** section.
- b) Click the name of the object type whose fields you want to modify (for example, SOXIssue).
- c) Expand the **Fields** section.
- d) Click **Add**.
- e) Select the fields to add to the profile and click **Done**.
- f) After it is added to the list of fields, click the field name.

The **Profile Field Configuration** panel opens. On this panel, **Display Type** is set and cannot be changed. Depending on the field type, additional fields might be available. For example, for user fields, the following fields can be set:

- **Include Disabled**
- **Starting Group**
- **Minimum Access** (Read, Write, Delete, Associate).

- g) Click **Done**.

4. In the Standard UI:

- a) From the **Object Types** table listing, click the name of the object type whose fields you want to modify (for example, SOXIssue).
- b) On the **Object Fields** table, click **Include**.
- c) On the **Available Object Fields** page, select the box next to the name of each object field you want to include.
- d) Click **Include**.

The included object field now appears in the list of available fields for this object type in this profile.

- e) Optional: Configure the object field in a view. Depending on the view, see either [“Navigational Views” on page 323](#) or [“Configuring fields in Detail and Activity views” on page 344](#).

Excluding fields from an object type

Excluding an object field from an object type in a profile immediately removes that object field from the views in which it is used, and that field is no longer available for configuration in a view or to users who are assigned that profile.

The availability of a field for configuration within any view depends on whether or not that field is included or excluded in the object type for that profile. Including or excluding fields for object types in one profile does not affect object-type fields in other profiles.

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
Or, in the Standard UI, click **Administration** > **Profiles**.
2. Click the name of a profile.
3. In the Task Focused UI:
 - a) Go to the **Object Types** section.
 - b) Click the name of the object type whose fields you want to modify (for example, SOXIssue).
 - c) Expand the **Fields** section.
 - d) Select the fields to exclude from the profile and click **Remove**.
 - e) Click **Remove** again to confirm.
4. In the Standard UI:
 - a) From the **Object Fields** table, select the box next to the name of each object field you want to exclude.
 - b) Click **Exclude**.
 - c) Click **OK** to remove the fields from the selected object type.

Results

The excluded object fields are now absent from the list of available fields for this object type in this profile.

Setting a field in a profile to required or optional

You can set a specific field to required or optional for a profile and object type.

Setting a field to required in a profile affects only the users who are assigned that profile.

Note: If a field is not listed in the **Object Fields** pane, you must include it before you can modify it (see [“Including fields in an object type”](#) on page 306).

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
Or, in the Standard UI, click **Administration** > **Profiles**.
2. Click the name of a profile.
3. Go to **Object Types**.
4. Click the name of the object type that has the field to modify.
5. In the Task Focused UI:
 - a) Go to the **Fields** section.
 - b) Click the name of the field to modify.
The **Profile Field Configuration** panel opens.
 - c) Set **Required** to True or False.
 - d) Click **Done**.
6. In the Standard UI:
 - a) In the **Object Fields** pane, click the name of the field to modify (for example, "Description").
 - b) On the **Object Field Information** pane for the selected field, click **Edit**.
 - c) In the **Required** field on the edit page, either enable the option to set the field as required or disable it.
 - d) Click **Save**.

Setting the display order of object types (Standard UI)

With the exception of the Business Entity object type, you can modify the order in which object types are displayed in a profile.

When you change the number of the list order of an object type, the system dynamically updates all the object types (except Business Entity).

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table:
 - a) In the box under the **Order** column, change the order value of the object types as wanted.
The maximum value allowed in the Order field is 999.
 - b) Click **Update Order**.
The object types in this profile now appear in the new order.

Example

The current display order for the following object types is Business Entity 1, Process 2, Sub-Process 3, and Account 4.

However, if you want to display Account (instead of Process and Sub-Process) after Business Entity, set the order number of Account to 2. When you click "Update Order", the system automatically reorders the Process number to 3 and Sub-Process to 4.

Now, wherever these object types are found together in the application, they appear in the following order: Business Entity 1, Account 2, Process 3, and Sub-Process 4.

Chapter 12. Managing the Home page, views for objects, and display types

You can manage the display of the Home page, the views for each object type that is included in a profile, and the display types for simple strings, long strings, reporting fragments, and enumerated strings.

Home page

The Home page is the initial page that users see when they log on to the IBM OpenPages with Watson application.

The Home page supports a tabbed interface for displaying selected reports and information. For each profile, you can configure one or more tabs to personalize the information on the page for users who are assigned that profile.

Typically, the number and types of tabs you configure on a Home page will vary by profile and depends on the business needs of users. If the number of tabs on a Home page extend beyond the size of the current browser window, right and left arrows are automatically displayed so users can scroll horizontally through the tabs.

Except for the My Work tab and the Dashboard tab, a tab on a Home page displays the name of the configured report.

The type of tabs that can be configured on the Home page include:

- Cognos reports
- Cognos Workspace reports
- Cognos Analytics dashboards
- Cognos Analytics stories
- JSP Reports
- The My Work tab, which is a Home page tab provided by OpenPages with Watson that contains configured panes (sections of a page) for predefined lists, filtered lists, and embedded reports.
- The Dashboard tab, which is a Home page tab provided by OpenPages with Watson. Administrators can add tabs that are mandatory and cannot be deleted or altered by users. Users can add panes to the Dashboard tab for quick access to the tasks and information that they use most.

You can control the order in which tabs (including the Dashboard tab and My Work tab) are displayed on the Home page.

For example, a Testers profile might have the following tabs configured: "My Tests - Performer" (report) as tab 1, the My Work tab as tab 2, the Dashboard tab as tab 3, "Test Notifications" (report) as tab 4, and the "FCM Dashboard" (report) as tab 5.

Additionally, you can hide, show, add, or delete tabs from the Home page quickly and easily without interruption to users who are assigned that particular profile.

Note:

- In a first-time installation, by default, the My Work tab and the Dashboard tab are both enabled.
- A report (or report fragment) that is embedded in a tab on the Home page executes when a user:
 - First clicks the tab containing the report
 - Navigates away from the Home page to other menus and then returns to that report tab on the Home page
 - Logs off and then logs on to the application again

- Switching between multiple tabs on the Home page and then returning to the original report tab does not rerun the report. To refresh report data, you must click the Refresh icon on the report tab.
- If the My Work tab is empty of content (no panes are configured) but other tabs are configured for display on the Home page, then a message, similar to the following, is displayed on the My Work tab to users who are assigned that profile:

OP-50544: There is no information configured for display on this Home page tab. Please contact your System Administrator.

- If the My Work tab is empty of content (no panes are configured) and no other tabs are configured for display on the Home page, then a message, similar to the following, is displayed on the Home page to users who are assigned that profile:

OP-50536: There is no information configured for display on your home page. Please contact your System Administrator.

- The Dashboard tab on a users Home page displays any panels defined by the administrator plus any panels created by the user. Panels specified as mandatory by the administrator are not editable or removable.

Guidelines for selecting reports to run in tabs

To avoid performance issues and cluttering the Home page with too many tabbed reports, consideration should be given to determining:

- Which reports or dashboards are best related to the type of tasks or activities a particular group of users have to accomplish
- Which profile (or profiles) should contain these reports or dashboards
- Are any of the selected reports or dashboards already configured for display on the My Work tab. If so, should these be removed?

The layout of tabs on a Home page

The number of tabs displayed on a Home Page for a given profile has no set limit and will vary according to your users' business needs.

Figure 18 on page 310 shows the basic layout of tabs on a Home page.

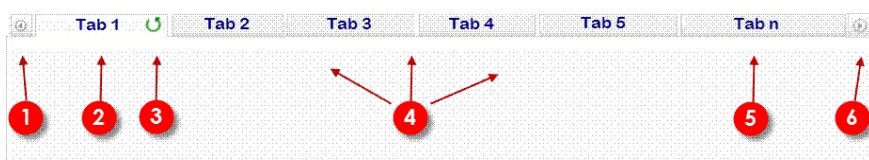


Figure 18. Layout of Tabs on a Home Page

Table 121 on page 310 contains a key to the previous illustration with a brief description of the various Home page elements.

Table 121. Description of Home Page Elements	
Key	Description
1	Left horizontal scroll arrow. If the number of tabs that are configured for a Home page do not fit in the browser window, an arrow is automatically displayed so users can scroll horizontally through the tabs.
2	Active tab. When multiple tabs are configured, only the currently selected tab is highlighted and becomes the active tab.

Table 121. Description of Home Page Elements (continued)	
Key	Description
3	Refresh icon. When clicked, refreshes the data on the selected tab.
4	Inactive tabs. Except for the My Work tab and the Dashboard tab, a tab typically displays the name of the configured report or dashboard.
5	"n" represents a number. There is no limit to the number of tabs that can be configured on a Home page.
6	Right horizontal scroll arrow. If the number of tabs that are configured for a Home page do not fit in the browser window, an arrow is automatically displayed so users can scroll horizontally through the tabs.

Configuring tabs on the home page

To configure tabs on the home page, use the **Home Page Tab Configuration** pane on the detail page of the selected profile.

Table 122 on page 311 describes the information displayed on the Home Page Tab Configuration pane.

Table 122. Columns on the Home page tab configuration table	
This column...	Displays this...
Name	The name of each configured tab. Typically, the name reflects the name of the selected report or dashboard. The My Work tab and Dashboard tab are the default Home page tabs provided by IBM OpenPages with Watson and are always displayed in the list.
Description	A brief description of the report, if available.
Status	The status of the tab. If the status is: - Visible - the tab is displayed on the Home page - Hidden - the tab is hidden from the Home page
Order	The position of the tab as it is displayed on the Home page. By default, the My Work tab is in position 1 and the Dashboard tab is in position 2. Note: Tabs that are disabled or hidden cannot be ordered and the box is not displayed.
Actions	The type of actions that can be used on a tab. The actions are: - Hide - hides the tab from display on the Home page - Show - unhides the tab and displays it on the Home page - Delete - permanently removes the tab from the list and Home page. Note: The My Work tab and the Dashboard tab cannot be deleted.

For information on localizing display text, see [“Localizing application text” on page 564](#).

Adding tabs for reports or dashboards

When you select one or more reports or dashboards for display in a tabbed format on the Home page, each selected report or dashboard is immediately:

- Displayed in a tab on the Home page of users who are assigned that profile.
- Listed under the **Home Page Tab Configuration** table on the Profile detail page.

Note: For details about configuring the My Work tab, see [“Configuring the My Work tab” on page 313](#).

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. On the **Home Page Tab Configuration** table, click **Add**.
4. From the list of reports and/or dashboards:
 - a) Expand a report folder to display a list of available reports.
 - b) Select the check box next to each report you want displayed in a tab on the Home page.

Note: Selecting multiple reports results in multiple tabs (one tab for each selected report).
 - c) Click **Add**.
5. Optional: Change the order in which tabs are displayed on the Home page (see [“Setting the display order of tabs” on page 312](#)).

Setting the display order of tabs

By default, the My Work tab is in position 1 on the Home page, the Dashboard tab is in position 2, and each tabbed report or dashboard that you add is displayed in the order in which it was added. During an upgrade installation, the Dashboard tab is hidden and at the bottom of the tab list.

You can change the order in which tabs (including the My Work tab and Dashboard tab) are displayed on the Home page. When you change the position of tabs on a Home page, the change is immediately reflected in the application user interface.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. On the **Home Page Tab Configuration** table, under the **Order** column, type over the existing number with the new number you want for positioning each tab on the Home page.
4. Click **Update Order**.

Hiding and un hiding tabs

You can control whether configured tabs are displayed or hidden from users in a profile. A tab that is disabled is hidden from users with the selected profile and can be unhidden by enabling it at a future time.

By default, newly added tabs are enabled and displayed to users who have the profile.

When you hide or unhide a tab, the following events occur:

- The value of the Status column changes for that tab.
- The value of the link toggles between **Hide** and **Show** depending on the selection.
- The tab is immediately hidden or unhidden from users on the home page of the selected profile.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. On the **Home Page Tab Configuration** pane, take one of the following actions in the **Actions** column:

Table 123. Home page tab configuration options	
To do this	Click
Hide a tab on the Home page for users of the selected profile	Hide in the row of the tab you want to hide.
Show a previously hidden tab	Show in the row of the tab you want to unhide.

Deleting tabs

When you delete a tab for a report or dashboard from a profile, the tab is immediately removed from the Home page of that profile, and from the list of tabs on the **Home Page Tab Configuration** table.

Note: You cannot delete the My Work tab or the Dashboard tab from the **Home Page Tab Configuration** table; you can only hide them.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. On the **Home Page Tab Configuration** table, under the **Actions** column, click the **Delete** link for the tab you want to permanently remove.

Configuring the My Work tab

The My Work tab is a default tab provided by IBM OpenPages with Watson, and contains the following panes (sections of a page) that can be configured in a profile for display to users:

- **Predefined Lists** - these panes display a list of predefined items that are tailored to the logged on user, such as My Checked-Out Files. Predefined lists also includes the My Reports pane, which can be configured with links to reports. For details, see [“Configuring predefined lists”](#) on page 314.
- **Filtered Lists** - these panes display a list of items based on a filter that you define for the selected object type. In addition, you can select object and/or report fragment fields (the data is displayed in columns), and set the order in which columns are displayed in the pane. For details, see [“Filtered lists on the My Work tab”](#) on page 314.
- **Embedded Reports** - each embedded report is displayed in a separate pane on the My Work tab. For details, see [“Configuring reports”](#) on page 316.

You can configure the default settings of the My Work tab for profiles. For more information, see [“Home page settings”](#) on page 625.

Note: The My Work tab can be enabled or disabled for a profile but cannot be deleted.

Note: If you disable the Filtered List View for an object type, the **View Details** link (or **Show All** link, in older versions) for that object on the **Home** page might open the wrong view.

Users can personalize the display and order of the panes on their My Work tab. You can control whether this functionality is enabled with the **My Work Home Page Can Be Personalized** setting. The default value is `true`. Upgrading does not change the sort order.

In a first-time installation, the My Work tab is enabled by default, but it is empty of content (no panes are configured), and a message, similar to the following, is displayed to users who are assigned that profile:

OP-50536: There is no information configured for display on your home page.
Please contact your System Administrator.

Configuring predefined lists

The following table lists the predefined lists that are available for display on the My Work tab.

Table 124. Available Predefined Lists	
This predefined list...	Displays this on the Home page...
My Checked-Out Files	a My Checked-Out Files pane that includes a list of files that were checked out by the logged on user.
Report Listing	a My Reports pane on the Home page for which you can configure links to reports. For embedded reports, see “Configuring embedded reports” on page 317 for details.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work Tab Configuration** table, click **Add Predefined Lists**.
4. On the **Available Predefined Lists** page:
 - a) Select the box next to each predefined list you want to display on the My Work tab.
 - b) Click **Include**. The included items are listed in the **My Work Tab Configuration** table.
5. If you selected Report Listing and want to populate the **My Reports** pane with a list of links to reports, see [“Configuring a My Reports listing”](#) on page 317 for details.

Filtered lists on the My Work tab

Filtered lists contain selected object type information based on the filter you defined for that object type.

Each filtered list that you configure is displayed in a table format within a pane on the My Work tab. For example, if you configured three filtered lists for the My Work tab, that tab would contain three separate panes - one for each filtered list.

Filtered lists can include one or more:

- Object fields
- Report fragment fields

Each field that you include in a filtered list is displayed as a column in that table.

For example, if you defined a filtered list for ineffective controls, and included (in addition to Name and Description) an object field for Classification and a report fragment field containing a Control Analysis bar chart, the table would display four columns (one for each field).

Note: By default, filtered lists on the My Work tab:

- Automatically include the Name and Description object fields.
- Use Reports as the name of the column heading for report fragment fields, and a clickable icon is displayed under the column for opening a single report fragment field. If multiple report fragment fields are configured for an object type, the icon displays a clickable down arrow with a selection list.
- Support only one column layout per object type. When multiple filtered lists are configured for the same object type, you cannot define different columns for display per filtered list on the My Work tab.

Example

For example, the Risk object type has filtered lists A, B, and C configured for display on the My Work tab. If the Name and Description fields were defined for filtered lists A and B, and an additional field, Domain, was the last field defined for filtered list C, then all the filtered lists, including A and B would include Domain for display on the My Work tab.

For each filtered list that you configure on the My Work tab for an object type, you can include or exclude fields, and set the order of columns in the table. If report fragment fields are configured, these are always the last column of the table.

When you configure a filtered list for display on the My Work tab, all filters that are defined for an object type are displayed in a selection list. After you select a filter, it no longer appears in the list of available filters.

The My Work tab supports only one column layout per object type. When multiple filtered lists are configured for the same object type, you cannot define different columns for display per filtered list on the My Work tab.

Configuring filtered lists on the My Work tab

You can configure filtered lists on the My Work tab for object fields or report fragment fields or both.

Note:

- A clickable icon is displayed for opening a single report fragment field under the Reports column. If multiple report fragment fields are configured for an object type, the icon displays a clickable down arrow with a selection list.
- If report fragment fields are configured, the Reports column, by default, is always the last table column and its column position cannot be changed.

Before you begin

Before you can configure a filtered list, you must have the following already defined for an object type:

- One or more filters for the selected object type. See [“Tasks to define filters for an object type” on page 267](#).
- Any report fragment fields and/or object fields that are in addition to the predefined standard IBM OpenPages with Watson object fields for that object type. See [Chapter 9, “Fields and field groups,” on page 199](#).

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work Tab Configuration** table, click **Configure Filtered List**.
4. On the **Select a Filter** page, select a filter from the list and click **Next**.
5. On the **Select Fields** page, do any of the following:

Table 125. Summary of Filter Actions	
Goal	Action
Include a field as a column in the filtered list	On either the Included Object Fields or Included Reporting Fragment Fields table, complete the following steps: a. Click Include. This opens a field selection page. b. Select the box next to each field you want to display as a column. c. Click Include.

Table 125. Summary of Filter Actions (continued)	
Goal	Action
Exclude a field as a column	On the Included Object Fields or Included Reporting Fragment Fields table, complete the following steps: - Select the box next to each field you want to remove as either a column or report. - Click Exclude.
Change the order in which object fields are displayed as columns	On the Included Object Fields table, complete the following steps: - In the Order column, change the order number of the field you want. - Click Update Order. When you change the number of a field, the system dynamically updates all the other numbers.
Include a field as a column that displays a report fragment	On the Include Reporting Fragment Fields table, complete the following steps: - Click Include. This opens a field selection page. - Select the box next to each report fragment field that you want to display. - Click Include.

6. Click **Finish**.

Editing filtered lists on the My Work tab

You can modify the fields in a filtered list and the order in which they are displayed.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work Tab Configuration** table, click the name of the filtered list table you want to modify.
4. On the table for included objects or report fragment fields, modify the information as necessary (for details, refer to Step 5 in [“Configuring filtered lists on the My Work tab”](#) on page 315).
5. Click **Finish**.

Configuring reports

You can use the following methods to configure reports on the My Work tab:

- **Report Listing** - this method creates a **My Reports** pane in which a list of selected reports can be displayed. Each listed report name is a link that, when clicked, opens the report in a separate window. For details, see [“Configuring a My Reports listing”](#) on page 317.
- **Embedded reports** - this method embeds each specified report in a separate pane on the My Work tab. For details, see [“Configuring embedded reports”](#) on page 317.

Note:

- Only published reports are displayed in the list of available reports (under the Cognos folder) for association on a My Work tab (either as a link in a list or as an embedded report). If you want to add a new report, you must first publish that report. For details, see [“Adding reports to OpenPages with Watson”](#) on page 171.

- Although JSP reports are available for selection as embedded reports on the My Work tab, only Cognos reports can be embedded (JSP reports cannot be embedded) on the My Work tab. A JSP report that is selected as an embedded report will result in a reporting error on the My Work tab.

Configuring a My Reports listing

You can configure links to reports in the My Reports pane on the My Work tab by either clicking the **Add Predefined List** icon or through the wizard by clicking the **Configure Reports** icon.

You can globally control the maximum number of reports that are listed on the My Work tab through the **Maximum Reports Listing** setting (for details, see [“Maximum reports allowed on the home page”](#) on page 627).

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work Tab Configuration** pane, take one of the following actions:

Table 126. My work table configuration options	
Option	Steps
Add Predefined Lists	On the Available Predefined Lists page, click Add Predefined Lists: a. Select My Reports b. Click Include. c. On the My Work Tab Configuration pane, click the My Reports link. d. Continue to Step 4. Note: If you already added a My Reports pane on the My Work tab but need to populate the list with reports, do not click the icon and skip directly to Step 4.
Configure Reports	In the Configure Home Page Reports wizard: a. In the Select Report Type step, select My Reports as the report type. b. Click Next. c. Continue to Step 4.

4. Click **Associate** to open the Reports list page.
5. On the **Reports** list page, select each report to include as a link in the **My Reports** pane. Then, click **Associate**.
6. Click **Finish**.

Configuring embedded reports

When you embed a report on the My Work tab, the report is displayed in a pane on the My Work tab of users who have the selected profile.

Use the following steps to embed reports on the My Work tab.

Note: You may need to modify the report to accommodate differences in the My Work tab display area and page targets. Make a copy of the report before you update the display details and targets to suit rendering within the My Work tab display area.

You can globally control the maximum number of embedded reports to show on the My Work tab through the **Maximum Embedded Reports** setting. For more information, see [“Maximum number of embedded reports on the home page” on page 626](#).

About this task

There are performance considerations when working with embedded reports. Although embedded My Work tab reports provide a convenient mechanism to present users with useful Cognos report data upon logon to IBM OpenPages with Watson, report execution times can vary depending on the report.

When configuring embedded reports, administrators should be careful not to configure the My Work tab with large or resource-intensive reports, as this will contribute to the overall load on Cognos resources. Some factors that can affect utilization of Cognos system resources include:

- The number of concurrent users logged on to the system
- The percentage of users executing reports or viewing computed fields
- The frequency with which users return to their respective Home pages

The following are some guidelines for configuring reports on the My Work tab:

- Only embed reports that are well-scoped and execute in less than <10 seconds for the typical application user.
- Configure no more than one (1) embedded report on the My Work tab for the majority of application users.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work Tab Configuration** table, click **Configure Reports**.
4. In the Configure Home Page Reports wizard:
 - a) In the **Select Report Type** step, select **Embedded Reports** as the report type.
 - b) Click **Next**.
5. On the **Choose Reports** step, click **Associate** to add reports to the list.
6. On the **Reports** page:
 - a) Select the box next to each report you want to embed in a pane on the My Work tab.
 - b) When finished, click **Associate** (you may need to scroll down to see the icon).

The selected reports are listed in the Associated Embedded Reports pane of the wizard.
7. If you want to remove any of the newly associated reports from the list (for example, a report was accidentally added), you can:
 - a) Select the box next to each report you want to remove.
 - b) Click **Disassociate**
8. Click **Finish**.

Modifying configured reports

Use the Configure Reports wizard to add or remove reports (both embedded reports and My Report links) from the My Work tab.

Note: You can also remove embedded reports from the **My Work Tab Configuration** pane. For more information, see [“Removing items from the My Work tab” on page 319](#).

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work Tab Configuration** pane, click **Configure Reports**.
4. In the **Select Report Type** field, select the report type that you want to modify.
5. On the **Associated Reports** page, take one of the following actions:

Table 127. Add or remove reports	
Task	Procedure
Add more reports	a. Click Associate. b. On the Reports list page, select each report to include. c. Click Associate.
Remove existing reports	a. Select each report to remove. b. Click Disassociate.

6. Click **Finish**.

Removing items from the My Work tab

You can remove previously configured tables (including embedded reports) from the My Work tab.

When a user with the modified profile either logs on to the application, refreshes or returns to the My Work tab on the Home page, the removed items may no longer be displayed.

Note: To remove links from the **My Reports** pane, see [“Modifying configured reports” on page 318](#).

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work Configuration** table listing:
 - a) Select the box next to each item you want to remove from the My Work tab.
 - b) Click **Disassociate**.

Configuring users' Dashboard tabs

The Dashboard tab allows users to create their own dashboard for their Home Page by adding panels and widgets. The configuration of a user's Dashboard tab is saved in the database and not in the web browser cache. This means that a user can clear the cache, switch to a different browser, or log in from a different computer without changing the configuration of the Dashboard tab.

Users can add new panels to their Dashboard tabs and for each panel add as many of the following types of widgets as needed:

- Filter Count widget, which appears in a user's dashboard panel as the object type name and a number representing the number of filters applied. When a user clicks the number of filters, the Filtered List

View page for that object type is opened. If a filtered list for that object type does not exist, then the Filtered List View page will not be opened.

- Object Global Search widget, which appears in the user's dashboard panel as the object type name followed by a search box. When a user enters a search term in the box, for example Accounts Receivable, the Search Results page provides a list of results.
- Static Web Link widget, which appears in a user's dashboard panel as a clickable link with the label that was provided for the widget. When creating this widget, users must begin the URL with the protocol, such as http://.
- Add New widget, which creates an **Add New** button that is preconfigured for a specific object type. Clicking the button, displays the Add New dialog box for that object type.

For each profile, administrators can add panels to a default Dashboard tab that is displayed for users who are logging on to OpenPages for the first time.

Administrators can specify that a panel is locked and cannot be changed by users. Administrators lock a panel by selecting the **Lock panel contents** check box in the **Create New Panel** window. When a locked panel is saved, it is automatically pushed to all users in the profile the next time they log into OpenPages. Administrators can also create panels that are unlocked, and these panels will be included in the default Dashboard tab for users who are logging on to OpenPages for the first time. Users can edit or delete unlocked panels in their own Dashboard tabs.

Both the Dashboard tab and the My Work tab will be present on a user's Home page unless specified as hidden by an administrator in the profile configuration. Clicking the Home button in the global header will return the user to either the Dashboard or My Work tab, depending on which tab was opened most recently.

Administrators can export the configuration of a default Dashboard tab in JSON format. This can be useful when migrating from one environment to another. For more information, see [“Exporting the configuration for a dashboard tab” on page 322](#).

Note: If the Global Search component is not enabled, then the Global Search widget is not available for users to add to their Dashboard tabs. If you disable the Global Search component for a profile, then any existing Global Search widgets are removed from users' Dashboard tabs the next time they log on to OpenPages. If you disable the Global Search component for an object type, then any Global Search widgets for that object type will be removed from users' Dashboard tabs. The Static Web Link widget type is always available, but the other widget types will only be available if users in the profile have access rights to the object type related to that widget type. If access rights are revoked for widget types that users have already placed on their Dashboard tabs, then those widgets will be removed the next time the users log on to OpenPages. Similarly, if the Add New capability is disabled for an object type that users have associated with a widget on their dashboard, then that widgets will be removed the next time the users log on.

Creating content for users' Dashboard tabs

For each profile, administrators can create content on a default Dashboard tab that is displayed for users who are opening the application for the first time. Administrators can also specify that a panel is locked. When a locked panel is saved, it is pushed to the Dashboard tab for all users in the profile and cannot be edited or removed by users.

Note: If the Global Search component is not enabled, then the Global Search widget is not available for users to add to their Dashboard tabs. If you disable the Global Search component for a profile, then any existing Global Search widgets are removed from users' Dashboard tabs the next time they log on to OpenPages. If you disable the Global Search component for an object type, then any Global Search widgets for that object type will be removed from users' Dashboard tabs. The Static Web Link widget type is always available, but the other widget types will only be available if users in the profile have access rights to the object type related to that widget type. If access rights are revoked for widget types that users have already placed on their Dashboard tabs, then those widgets will be removed the next time the users log on to OpenPages. Similarly, if the Add New capability is disabled for an object type that users

have associated with a widget on their dashboard, then that widgets will be removed the next time the users log on.

Procedure

1. Log on to IBM OpenPages with Watson as a user with the Profiles application permission set.
2. From the menu bar, select **Administration** and click **Profiles**.
3. Click the name of the Profile for which you want to create a default Dashboard tab.
4. From the menu bar of the Profiles detail page, click **Home Page Tab Configuration**.
5. In the Dashboard row, click **Edit**.
6. To add a panel, click **Create New Panel**.
7. In the **Create New Panel** window, type a title for the panel. The name for the panel must be unique. If a user in the profile already has a panel with same name, the name of the user panel is changed. For example, if you create a panel called My Panel and the user already has a panel by that name, the user panel is renamed to My Panel(1).
8. Under **Panel Widgets** select a widget type.

You can add as many widgets as you want by clicking the **Add New Widget** button and specifying the object type for each widget. The order of widgets in the panel can be changed by dragging them up or down.
9. When you are finished adding and arranging the order of widgets, click the **Create Panel** button.
10. To change the layout of panels in the default Dashboard tab, you can use drag and drop.
11. Click **Done Editing**.

Results

When you save a locked panel, it is pushed to the Dashboard tab of all users in the profile and will appear the next time that they log on to OpenPages. In order for the change to occur for all users in the profile, all users must log on to OpenPages after the profile change.

To edit or delete a panel, administrators and users can hover their mouse pointers over the panel and click the edit or delete icon. Users are not able to edit or remove locked panels. When users hover their mouse pointers over locked panels, the edit and delete icons are not available to them.

When you save a panel that is not locked, it appears only on the default Dashboard tab that users see when they open the application for the first time. Unlocked panels are not pushed to users' Dashboard tab. They can be edited or removed by users.

Editing the content of users' Dashboard tabs

For each profile, administrators can edit content on a default Dashboard tab that is displayed for users who are opening the application for the first time. Edits to the default Dashboard tab will not affect the Dashboard tab for existing users unless a panel is locked. If an administrator specifies that a panel is locked, then that panel is pushed to the Dashboard tab for all users in the profile and cannot be edited or removed by users.

Procedure

1. Log on to IBM OpenPages with Watson as a user with the Profiles application permission set.
2. From the menu bar, select **Administration** and click **Profiles**.
3. Click the name of the Profile for which you want to edit a default Dashboard tab.
4. From the menu bar of the Profiles detail page, click **Home Page Tab Configuration**.
5. In the Dashboard row, click **Edit**.

You can perform the following tasks:

- To add a new panel to the default Dashboard tab, click **Create New Panel**. For more information, see [“Creating content for users' Dashboard tabs” on page 320](#)
 - To edit an existing panel, hover your mouse pointer over the title bar of the panel and click the pencil icon. You can change the title of a panel by clicking the title and typing a new name.
 - To delete a panel, hover your mouse pointer over the title bar of the panel and click the trash can icon.
 - To make a panel mandatory for all users in the profile and push it to their Dashboard tab, select the **Lock Panel Contents** check box. When you save the panel, it is pushed to users' Dashboard tabs and will appear the next time that they log on to OpenPages, and users will not be able to edit or remove it. Panels that are not locked can be edited and removed by users.
6. Click **Done Editing**.

Exporting the configuration for a dashboard tab

Administrators can export the configuration of a default Dashboard tab in JSON format. This can be useful when migrating from one environment to another.

Procedure

1. Log on to IBM OpenPages with Watson as a user with the Profiles application permission set.
2. From the menu bar, select **Administration** and click **Profiles**.
3. Click the name of the Profile for which you want to export the configuration of the default Dashboard tab.
4. From the menu bar of the Profiles detail page, click **Home Page Tab Configuration**.
5. In the Dashboard row, click **Edit**.
6. Click the **Download JSON** button, and open the JSON file in a text editor.

If the Dashboard tab uses multibyte characters, you must use a text editor that supports UTF-8, such as Notepad or Microsoft Word. If you open the JSON file in Microsoft Wordpad, the multibyte characters might not display correctly.

Configure views for objects

For each object type that you include in a profile, you can configure various views of data for that object. A view displays information about an object type in different formats and provides a means for customizing and filtering information on a page for objects and custom form objects.

The following list summarizes the standard views that you can configure. IBM OpenPages with Watson categorizes views as follows:

Navigational Views

- Overview Pages
- Folder View
- Filtered List View
- Grid View

Object Views

- Detail View
- Activity View

Association Views

- List View
- Context View

Creation Views

Note: If you enable a navigational view for the Process Diagram, Data Input, or Data Output object type, it is not available as a menu item for users who are associated with that profile. These objects are available only in the context of a Process.

For information about configuring specific object types in a profile, see [“Including object types in a profile”](#) on page 304.

Fields that you configure for a specific object type and view page are displayed to users who have that profile, and fields that you exclude from that object type and view are hidden from users.

Fields can be object fields, computed fields, and report fragment fields.

When you modify an object view for a particular object type (including custom forms), the change is immediate and displays everywhere the object type appears in a table within the OpenPages with Watson application. Changes that you effect for one profile do not result in changes to other profiles.

For example, you create two new fields for the Risk object type and want to display these fields to users with the Manager profile on the detail page of Risk objects. You open the Manager profile, select the Risk object type from the list, select the Detail view page, and then choose the new fields to include on the Detail view page. When users with the Manager profile view, create or modify a risk, the two new fields will be displayed on a Risk Detail view page. For users who have a different profile (not Manager), the new Risk fields are hidden unless you also include these fields in that profile.

Navigational Views

Navigational Views assist users in finding instances of specific objects.

Navigational views include the following view types:

- Overview
- Folder
- Filtered List
- Grid

When you add, remove, or modify Navigational Views in a profile for a specific object type, consider the following items:

- Views can be enabled or disabled.
 - Note:** If you disable the Filtered List View for an object type, the **View Details** link (or **Show All** link, in older versions) for that object on the **Home** page might open the wrong view.
- Some views can be deleted.
- Most views, except Overview pages, can be reordered.
- The **Bulk Update** feature can be used with grid views because grid views contain editable fields.
- Users with the assigned profile who are already logged on to the application must log out and log in to see the changes.
- Users can change the sort order and field order in Filtered List Views and Grid Views.
- Users cannot add the primary parent hierarchy or business entity hierarchy fields to a Navigational View for any object type.

Overview pages

An Overview page displays a hierarchical object-tree view of an object type. For example, if you wanted to include an Overview page for Control Objectives, you could do so through a profile.

As an administrator, you can:

- Control which object types are included or excluded in the object-tree hierarchy on an Overview page (see [“Including object types on an overview page”](#) on page 333 and [“Excluding object types from an overview page”](#) on page 334 for details)

- Enable or disable an Overview page for an object type (see [“Configure views for objects” on page 322](#) for details)

An Overview page is not supported for the following object types: SOXProject, SOXDocument, SOXExternalDocument, SOXMilestone, SOXIssue, SOXTask, SOXSignature, and ProjectActionItem.

Folder views and Filtered List views

A **Folder view** displays a page view of folders (including sub-folders) containing the selected object type. The information is displayed in columns on the page.

A **Filtered List view** displays a page with search filter options that you can use to display objects of the same type that match your search criteria. First, select the object type to view. Then, select the **Filtered List view** from the Filter selector. The view is then populated with objects that match the filter criteria. Use this view to display filter objects of the same type that match the search criteria in the filter the user selects. The user can personalize the display of a Filtered List view and limit what fields of information are displayed.

For Filtered List and Folder views:

- The **Name** field is required. Always configure it in the first column.
- If report fragment fields are configured, the Reports column is always the last column in the table. The position of the Reports column can be changed in Grid View.

Example

If you previously disabled the Folder view and Filtered List view pages for Control Objectives in a profile, and you want to make that object type and its children directly accessible again through the Assessments menu to users who are assigned that profile. You could enable the Folder view and/or Filtered List view for the Control Objective object type. Enabling either view page would cause the Control Objectives menu item to be dynamically displayed on the Assessments menu. However, only the view page that was enabled would be displayed when the menu item was selected. If you enabled both view pages, you could set, for example, the Filtered List view page to be displayed first to users.

As an administrator, you can perform the following functions:

- Control which fields are displayed as table column headings in a Folder or Filtered List view (see [“Navigational Views” on page 323](#))
- Set the order in which table column headings appear (see [“Setting the display order of fields in a view” on page 329](#))
- Enable or disable a Folder or Filtered List view page for an object type (see [“Configure views for objects” on page 322](#) for details)
- Control which view page (Folder or Filtered List view) is displayed first to users when both views are configured (see [“Setting a default view” on page 329](#) for details)
- Control whether users can edit fields in the Filtered List view ([“Editable fields in a Filtered List View” on page 632](#) for details)

Grid views

The grid view allows you to select how information about an object is displayed by selecting an option from the View selector.

A grid view allows users to view, compare, and edit fields from up to three different object types in one location. A grid view allows users to perform operations on multiple objects at the same time. Additionally, users can personalize the information by modifying the fields that are displayed, field order, sort criteria, and column widths.

The grid view allows users to move between the display of objects fields in full mode and compact mode. This ability allows the user to show all configured fields for an object or display only the subset that you

select. You define the objects that are displayed on a grid view. Users can then select a grid view and edit the fields in the view, including reordering columns of information.

Use the **Grid Actions** menu to create an item, update multiple items (bulk update), export information, delete, lock, and unlock.

The grid view provides access to an Info Card. The card displays the values for all configured fields for an object type.

If users are allowed to edit fields in an object, define a grid view. Because grid views have editable fields, you can use the **Bulk Update** feature.

For information about creating grid views, see [“Creating a Grid view ” on page 335](#)

Object views

Object Views provide detail instance data for an object.

Object Views include the following view types:

- Detail
- Activity

When you add, remove, or modify Object Views in a profile for a specific object type, users with the assigned profile who are already logged on to the application may have to refresh the page to see the changes. Object views can be enabled or disabled. Some object views can be deleted.

Detail views

A **Detail View** displays data on the same page for the selected object including fields and any associations it has to other objects.

From an object's Detail page, application users can edit and/or view object-specific fields for the selected object, and add or associate other objects to it. You can configure the **Detail View** or any **Activity View** to be the page that users see by default when they click the linked name of an object from an Overview, Folder, Filtered List, or List View page.

Fields can be object fields, computed fields, and report fragment fields.

Note:

- The Detail view is required for objects and custom forms and can be disabled but not removed. When you add a new object type to the Default profile, a Detail view is automatically configured for that object type.
- When users export data from a Filtered List View to a spreadsheet, the data that is directly exported corresponds to the fields that are configured in a Detail view for the selected object type with the exception of Long String fields that have a large subtype. Fields with a large subtype are ignored by Export and FastMap as these fields might be too large to be stored in a cell (the maximum storage for a cell is 32 KB).

As an administrator, you can:

- Control which fields are displayed in the table rows of a Detail view (see [“Configuring fields in Detail and Activity views” on page 344](#))
- Set the display order of the fields (see [“Setting the display order of fields in a view” on page 329](#))
- Set specific fields to be view only or editable (see [“Setting object fields as read-only or editable” on page 347](#))
- Set specific fields to span the 2-column table layout of the Detail page (see [“Spanning table columns” on page 347](#))
- Insert section headings on a page to delineate a set of fields (see [“Inserting section headings” on page 346](#))

- Configure how report fragment fields are displayed to users (see [“Configuring the display type for reporting fragment fields \(Standard UI\)”](#) on page 348)
- Configure how string data is displayed to users (see [“Configuring display types for simple string fields \(Standard UI\)”](#) on page 349)
- Configure whether the fields in a **Detail View** or in a user profile are available for creating an **Advanced Filter** on a **Filtered List View** page (see [“Advanced filters field configuration for Filtered List View”](#) on page 629)

Activity views

Activity Views are multi-object views focused on performing a specific task, such as control assessments. An Activity View page provides a way for users to concurrently view and edit specific fields for an object, including any child objects that have been defined for this view, with minimal navigation.

An Activity View can display up to three levels of objects (the current object, list and detail panes for child objects, and objects under a selected child object).

You can create your own Activity View pages for an object type in which users can edit, view, and manage multiple associated objects on the same page. Depending on the view type, information is displayed as either a page (such as a Folder View or Detail view page) or in a section of a page (such as a Context pane). By default, an Activity View is enabled and is automatically added to the list of views that can be selected from the **Current View** selection on the object’s detail page. Users who are assigned the selected profile have immediate access to the new Activity View.

In an Activity View, you can choose child object types at any level in the hierarchy for display in an Activity View. For example, if users need to determine the effectiveness of a particular control, you could select **Control** and **Test Result** (skipping the **Test** object) under a **Risk** object so only objects relevant to performing the task are displayed in an Activity View. You can also sort how object types are displayed and select paths to scope or limit the objects that are returned.

For more details on using Activity Views, see [“Creating Activity Views”](#) on page 337.

As an administrator, you can:

- Create, modify, or delete Activity Views (see [“Creating Activity Views”](#) on page 337)
- Control which fields are displayed in the table rows of an Activity View (see [“Configuring fields in Detail and Activity views”](#) on page 344)
- Set the display order of the table rows containing the fields (see [“Setting the display order of fields in a view”](#) on page 329)
- Set specific fields to be view only or editable (see [“Setting object fields as read-only or editable”](#) on page 347)
- Set specific fields to span the 2-column table layout of the activity page (see [“Spanning table columns”](#) on page 347)
- Insert section headings on a page to delineate a set of fields (see [“Inserting section headings”](#) on page 346)

Association views

Users with the assigned profile can use Association Views to view a page that displays parts of another pages.

Association Views include the following view types:

- List
- Context

When you add, remove, or modify Association Views in a profile for a specific object type, users with the assigned profile who are already logged on to the application may have to refresh the page to see the changes.

List views

A **List view** displays objects of the same type in a list format, with objects listed in ascending order. Depending on the object type, list views can be displayed as either a page or a pane.

By default, list views are displayed as pages for the following object types: Business Entities (SOXBusEntity), Milestones (SOXMilestone), Milestone Action Items (SOXTask), and as panes on a Detail view page for listing associated parent or child objects.

If you have a Folder or Filtered List view for Business Entities, the default list view for this object type is not used.

When you configure either a Folder or Filtered List view for Business Entities (SOXBusEntity), the default list view for this object type is not used.

For list views:

- You cannot add a list view to a custom form object or remove a list view from an object.
- The **Name** field is always displayed in column 1 and its position cannot be changed.
- If report fragment fields are configured, the Reports column is always the last column in the table and its position cannot be changed.

As an administrator, you can:

- Control which fields are displayed as table column headings in a list view.
- Set the display order of the table column headings.

Context panes

A Context pane appears in the Detail page for an object and provides information about the object that is the focus of the Detail page. When you are looking at the details of associated objects, use the Context pane to remind you of the key information about the object that is the focus of the Detail page.

For example, you could use a Context pane to include System Fields such as, Business Entity Structure and Primary Association Path, or a report fragment field that displayed a line chart showing trends.

As an administrator, you can:

- Control which fields are displayed in a Context pane (see [“Including and excluding fields in navigation and association views”](#) on page 332)
- Set the display order of the fields (see [“Setting the display order of fields in a view”](#) on page 329)

Creation views

Creation views allow you users to add new objects using the Add New wizard.

In previous releases, the layout of the Add New wizard was driven by a single view definition, either an Activity View that is named Add New, or the Detail view. There was also no way to associate existing child objects to the object that is being created without a separate step.

Now, a category of view that is called Creation views allows the definition of multiple Add new view definitions for a single object type for a single profile.

For more information on using Creation views, see [“Creating a Creation view”](#) on page 343

Enabling a view

The process of enabling a view for an object type in a profile is the same for Navigational and Object Views. It does not apply to Association Views.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).

2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type (for example, SOXControl) for which you want to enable a view.
4. Navigate to the type of view you want (such as **Navigational Views** or **Object Views**).
5. Click the **Enable** link under the **Actions** column in the row containing the particular view you want to enable.

Note:

- The link changes from **Enable** to **Disable**.
 - The value in the Enabled column changes from false to true.
6. Optional: Configure the selected view:
 - To add or remove object types for display in an object-tree hierarchy on an Overview page, see [“Including object types in a profile” on page 304](#) for details.
 - To add or remove fields for a specific view, see [“Removing object types from a profile” on page 305](#).
 - To control which view is displayed first to users when multiple views for a page are configured, see [“Setting a default view” on page 329](#) for details.
 - To associate a filter that will narrow the scope of data that is returned from a Filtered List view page, see [“Associating filters to Filtered List view and Grid view pages” on page 334](#) for details.

Disabling a view

The process of disabling a view for an object type in a profile is the same for Navigational and Object Views. It does not apply to Association Views.

About this task

- For **Overview** views - when you disable an Overview for an object type, the Overview menu item that corresponds to that object type is dynamically removed from the menu list.

For example, if you enabled a Control Objectives Overview page and then decided you no longer wanted it, you could remove the Overview page for that object through the profile. When you disable the Overview view, the Control Objectives Overview menu item would be dynamically removed from the Assessments menu list for all users who are assigned that profile.

- For **Folder View**, **Filtered List View**, and **Grid View** - when you disable these views, the corresponding menu item with the name of the object type, is dynamically removed from the menu list for all users who are assigned that profile. Although the object type and its children are still accessible from other view pages, the object type would no longer be directly accessible to users from a menu.

For example, if you disabled both the Folder View and Filtered List view pages in a profile for the Process object type, application users who were assigned that profile would still be able to access Process objects from a Process Overview page, a Business Entity Overview page, or the detail page of a parent or child object. However, the Processes menu item would be removed from the Organization menu.

Note: If you disable the Filtered List View for an object type, the **View Details** link (or **Show All** link, in older versions) for that object on the **Home** page might open the wrong view.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type (for example, SOXControl) for which you want to disable a view.
4. Navigate to the type of view you want (such as **Navigational Views** or **Object Views**).

5. Click the **Disable** link under the **Actions** column in the row containing the particular view you want to disable.

Results

- The link changes from **Disable** to **Enable**.
- The value in the Enabled column changes from true to false.

Setting a default view

On pages where multiple views are enabled for an object type, you can select which view you want as the default view for that page. The process of setting a default view for an object type in a profile is the same for Navigational and Object Views that contain a Make Default link. It does not apply to an Overview view or Association Views.

For example, if you have a Grid View, Folder View, and Filtered List View enabled for Control object types, you could set the Grid View page to display first when users select **Control** from the **Assessments** menu.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type (for example, SOXControl) for which you want to set a default view.
4. Navigate to the type of view you want (such as **Navigational Views** or **Object Views**).
5. Click the **Make Default** link under the **Actions** column in the row containing the particular view you want to display as the default view.

Note:

- The **Make Default** link is removed from the selected view.
 - The value in the Default column changes from false to true.
6. To view the changes to the default view, users must log out and log back in to the application.

Results

If you later decide to change the default view to another view, click the **Make Default** link in the row containing the view you want to display as the default view.

Setting the display order of fields in a view

You can dynamically change the order in which fields are displayed for object types in a view.

Fields can be object fields, computed fields, and report fragment fields.

Note: The following field limitations apply only to **Filtered List**, **Folder**, and **List** views:

- The **Name** field is always displayed in column 1 and its position cannot be changed.
- If report fragment fields are configured, the Reports column is always the last column in the table and its position cannot be changed.

When you reorder fields in a view, the change is immediately displayed to all users.

The process of setting the display order of fields for an object type in a profile is the same for all views.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).

2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type you want to modify.
4. Select one of the following views and complete the steps identified:

Table 128. Views	
Navigate to this tab...	To select a link for this view...
Navigational views	Folder, Filtered List, or Grid If Grid Views are defined, click the name of a grid view link, and then click Next until the Specify Field Settings screen is displayed in the Grid View wizard.
Association views	List or Context
Object views	Detail or Activity. If Activity Views are defined, click the name of an activity view link, and then click Next until the Specify Field Settings pane is displayed.

5. On the **Included Object Fields** table, locate the field to change:
 - a) In the **Order** field in the row of the selected field, type the new display order number for that field.
 - b) Click **Update Order**.
 - c) For **Detail Views** only - click **Save** to save your changes and return to the object type detail page.
 - d) For **Activity Views**, click **Next** and **Save**.
 The fields are automatically reordered as specified.
 - e) For **Grid Views**, click **Save**.
 The fields are automatically re-ordered as specified.

Example

If the "Classification" object field on the property table of a Risk object Detail View page is in position 9 on the list and you wanted it to precede the "Location" object field, which is in position 3, you would change the display order number for the "Classification" field from 9 to 3. All the other object fields after position 3 are automatically re-ordered - so the display order for the "Location" field would become 4, the next field that followed would become 5, and so forth.

Copying views for an object from one profile to one or more other profiles

You can copy the object views (Detail View and Activity View) and creation views for an object from one profile to one or more other profiles.

About this task

To access the **Profiles** menu item, you must have the **Profiles** application permission set on your account. For more information, see [“Types of application permissions” on page 91](#).

Before you copy a view, keep the following points in mind:

- If an object in the source profile is missing from the target profile, the copy operation will not be successful.
- If fields, field groups, or filters in the source profile are missing from the target profile, they will be added to the target profile by the copy operation.
- Field properties for the object that you selected, such as display type and whether a field is required, are retained when the copy operation is complete. When fields are added to the target profile by the copy operation, they have the same properties as they have in the source profile.

- Fields that are related to the view but not included in it, are not automatically added to the target profile by the copy operation. For example, suppose that the view that you are copying has dependent fields. Unless the view also includes the controlling fields, the dependent fields are not copied to the target profile. As a result, the user of the target profile might have no way to set the value of the controlling fields, and dependent field behavior (Visible, Required, or Editable) might not work as expected. If the view you are copying has any controlling fields that are not included in the view, you should first determine whether those fields are included in the target profile. If they are not, determine whether you want to manually add them to the target profile. For more information, see [“Modifying controllers for a dependent field \(Standard UI\)”](#) on page 282 and [“Configuring dependent picklists”](#) on page 288.
- If the view already exists in any of the target profiles, and you proceed with the copy, the existing view in the target profile is overwritten by the copied view. If the overwritten view was disabled or set as the default view in the target profile, it is still disabled or set as the default view when the copy operation is complete. The order of the overwritten view does not change in the target profile.
- If a view with the same name but of a different view type exists in the target profile, the view is not copied.
- Filters that are associated to the source view are copied to the target view. If you want the filters to be available in the Filtered List View or Home page in the target profile, you must manually add them. For more information, see [“Tasks to define filters for an object type”](#) on page 267.

<https://youtu.be/CrF69RUe4bk>

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode”](#) on page 71).
2. Click **Administration > Profiles**.
3. Click the name of the source profile that includes the object with the view that you want to copy.
4. Click the name of the object that you want to copy views to.
The **Profile** page for the object opens.
5. Click the **Object Views** or **Creation Views** tab, depending on which type of view you want to copy.
6. Click the **Copy** link beside the source view that you want to copy.
7. Select one or more target profiles to copy the source view to.
8. Click **Validate** to verify that the object types and fields exist in the target profiles that you selected.
The **Validate** tab shows any warnings and errors.

- If there are no issues, a checkmark  is displayed.
- If fields, field groups, or filters that are in the source profile will be added to the target profile, an information message  is displayed.
- If the view already exists in any of the target profiles, a warning  is displayed.
- If an object in the source profile is missing from the target profile, an error  is displayed.

9. Click **Copy**.
10. Click **Done**.

The **Results** tab displays the results of the copy operation.

- If the copy was successful, a checkmark  is displayed. The view is copied to the target profiles that you selected.
- If the copy was unsuccessful because one or more objects are missing from the target profile, an error  is displayed.

11. Disable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71](#)).

Including and excluding fields in navigation and association views

For each **Folder**, **Filtered List**, **List View**, **Grid View**, and **Context** pane that you configure for an object type within a profile, you can include, exclude, and set the order of fields. When you include or exclude object fields in a Folder, Filtered List, List, Context, Activity, or Grid view, the change immediately affects all users who are assigned that profile.

Fields can be object fields, computed fields, and report fragment fields.

Each object type has a set of predefined object fields that consist of both shared and object-specific fields. The shared object fields (such as *Name*, *Description*, *Created By*, and so forth) are common to all object types and belong to the System Field field group. With the exception of the **Name** field, which is required and always in position 1, you can choose which system and object-specific fields to include or exclude from an object view. In addition to object fields, you can also include report fragment fields that you define. In this way, you can tailor each view to accommodate changing business needs.

Note:

- For Overview pages, see [“Including object types on an overview page” on page 333](#) and [“Excluding object types from an overview page” on page 334](#) for details.
- For Detail and Activity view pages, see [“Configuring fields in Detail and Activity views” on page 344](#) for details.

For information and examples about these views, see the following topics:

- **Filtered List and Folder views** - see [“Folder views and Filtered List views” on page 324](#)
- **List views** - see [“List views” on page 327](#)
- **Context panes** - see [“Context panes” on page 327](#)
- **Grid views** - see [“Folder views and Filtered List views” on page 324](#)

Including fields in views

Before you can include an object field or reporting fragment field in a Navigational or Association view, the field must be visible in the object field or reporting fragment table listing for the selected object type or custom form. If the field is part of a field group, make sure you include the field group for the selected object type.

For details, see [“Including fields in an object type” on page 306](#).

When you include object fields or reporting fragment fields in a Navigational or Association view for the selected object type, the fields are displayed as table column headings in that view. By default, the column heading for reporting fragment fields is called Reports.

About this task

For List and Folder views, the user cannot adjust the column width or configure which columns will appear. It is a good practice to limit the number of columns you configure for those views.

For Grid and Filtered List views, the user can adjust the column width and can configure which columns are visible.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).

4. Select the view that you want.
5. To add field columns to the selected view:
 - a) On either the **Included Object Fields** or **Included Reporting Fragment Fields** table, click **Include**. The available fields selection page is displayed.
 - b) Select the box next to each field you want to display.
 - c) Click **Include**.
6. To modify the order in which the fields are displayed in columns in a Navigation or Association View, see [“Setting the display order of fields in a view” on page 329](#).

Excluding fields from views

When you exclude object fields or report fragment fields from either a Navigational or Association View for the selected object type, the fields are removed from the table column headings in that view page.

With the exception of the required **Name** field, you can exclude any field from an object view. For example, if you exclude the Description object field from a Filtered List View for an object type, the Description table column and its associated data are dynamically removed from the Filtered List view page and the change is immediately visible to all users.

Note: If you exclude object fields that are referenced by JSP reports, the report may fail or return unexpected results.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. Select the view that you want.
5. To remove object field columns from the selected view:
 - a) From either the **Included Object Fields** or **Included Reporting Fragment Fields** table, select the box next to each object field you want to remove.
 - b) Click **Exclude**.

Including object types on an overview page

When you include an object type for display in the object-tree hierarchy on an Overview page, the following occurs:

- The object type and any associated child object types are dynamically displayed to users (who are assigned that profile) in the object-tree hierarchy.
- The modification is effective immediately and there is no need to restart any IBM OpenPages with Watson services.

You can optionally display the Description column on an object’s Overview page by modifying its object view information. The Name column is required and cannot be hidden.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. On the **Navigational Views** table of the selected object type, click the **Overview** link.

5. On the **Included Object Types** tab, click **Include**.
6. On the **Available Object Types** page:
 - a) Select the box next to each object type you want to include in the object-tree hierarchy.
 - b) When finished, click **Include**.
7. To show or hide the Description column on the Overview page:
 - a) On the **Object View Information** tab, click **Edit**.
 - b) Click the **Show Description** arrow and select either:
 - **True** - to display the Description column.
 - **False** - to hide the Description column.
 - c) Click **Save**.

Excluding object types from an overview page

When you exclude an object type from display in the object-tree hierarchy on an Overview page, the following occurs:

- The object type and any associated child object types are dynamically removed from users (who are assigned that profile) in the object-tree hierarchy - think carefully before removing an object type from an Overview page.
- The modification is effective immediately and there is no need to restart any IBM OpenPages with Watson services.

For example, if you exclude Controls from the Business Entity Overview page, the Control object - including any associated object types - will no longer be displayed when you expand the object-tree hierarchy on the Business Entity Overview page. The OpenPages with Watson structure will appear to stop at the Risk level. In addition, Tests and Test Results will no longer be displayed, since the Controls they are associated with are hidden and not visible on the Business Entity Overview page.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** tab:
 - a) Select the box next to each object type you want to exclude from the Overview page object-tree hierarchy.

Note: Excluding an object type also hides its children. For example, if you exclude Risks from the Overview page, Controls, Tests, and Test Results will also be hidden from view. You do not need to select each type - only the parent object type.
 - b) Click **Exclude**.

Associating filters to Filtered List view and Grid view pages

When you associate a filter to a Filtered List View or a Grid View, the filter is displayed in the filter selector for that object type. By using a filter, you can narrow the scope of data that is returned in a Filtered List View or a Grid View for users who are assigned a specific profile.

Important: Before you can associate an object-specific filter to a Filtered List view or Grid View page, you must create a public filter for that object type by following the instructions in [“Tasks to define filters for an object type” on page 267](#).

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.

3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. Under the **Navigational Views** table of the selected object type, click the **Filtered List** link.
5. Complete the following actions:
 - a) On the **Associated Filters** tab, click **Associate**. The filters selection page is displayed.
 - b) Select the box next to each filter that you want to include.
 - c) Click **Include**.

Disassociating filters from Filtered List view and Grid view Pages

If you have a filter that is no longer appropriate for display in the filter selector on a Filtered List view page or a Grid view page for an object type, you can remove it from the list.

Procedure

1. Access the **Profiles** page (see “Accessing profiles” on page 298).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type (for example, SOXControlObjective) that has the filter you want to remove.
4. From the **Associated Filters** table listing, select the box next to each filter you want to disassociate from this view.
5. When finished, click **Disassociate**.

Creating a Grid view

In IBM OpenPages with Watson, you can create a grid view of an object for the users who are assigned to a profile. You specify the fields that are editable so that users can perform a certain task, such as entering KRI values or performing a self-assessment update. Additionally, you can provide guidance in the grid view to these users.

About this task

The process of creating a grid view includes the following steps:

- Provide details about the grid view.
- Optionally, select the related objects that contain fields of information that the user will require to perform the task.
- Specify the settings for the object types.
- Configure fields for the grid view.

Procedure

1. Click **Administration > Profiles** and select a profile.
2. Select the object that will be at the root of the grid view.
3. Under **Navigational Views**, click **Add New**.
4. To provide details about the new grid view, complete the following actions:
 - a) Add a name and description. Optionally, enter the translations for the name. The description is for administrators only.
 - b) Add guidance to the users who are assigned to the profile, such as the methodology that the users should follow in performing the task. You can format the text.
 - c) If the grid view is not ready for users to access now, clear the **Enabled** check box. The new grid view is enabled by default.
 - d) Click **Next**.

5. If you want to select the related objects that contain fields of information that the user will require to perform the task, complete the following actions:
 - a) Click **Choose Object Type**.
 - b) Select an object type for the selected object.
 - c) Click **Apply**.
 - d) Repeat these steps for each object that you want to add.
 - e) When you have added all the related objects, click **Next**.

The related objects do not have to be direct child objects. You can skip levels. For example, the object model may be Process --> Risk --> Control --> Test Plan --> Test Result. You create a grid view that is Process --> Control --> Test Result.

If you do not want to include related objects, just click **Next**.

Note: Descendants of recursive object types, such as Business Entity, appear under all of their ancestors, not just the most immediate ancestor. For example, if the path is set to Business Entity/Preference and the hierarchy of objects is North America Division/US Region/Pref1, Pref1 appears as a descendant of both North America Division and for US Region.

6. If there are at least two paths between the selected objects, select one or more paths that you want to use.
7. To specify the sort criteria for the object, complete the following actions:
 - a) Click **Specify Sort Criteria**.
 - b) Click or Ctrl+click the fields and click the double arrow (>>).
 - c) To change the order in which the fields appear, select the field and use the up arrow or the down arrow.
 - d) To change how the fields are sorted, select each field and click the up triangle or the down triangle.
 - e) Click **Apply**.
8. To apply a filter to the objects, complete the following actions:
 - a) Click **Choose Filter**.
 - b) Select a filter that was created for this object.
 - c) Click **Apply**.
9. Click **Next**.
10. To configure fields for the grid view, complete the following actions:
 - a) To select the fields that will be displayed, click **Choose Fields**, select the fields, and click **Apply**.
 - b) To allow your users to control which fields are available in the grid view, select **Full Mode** to see the field available in the grid view for an object.

Compact Mode is a subset of the fields that appear in Full Mode. For example, your users may want to hide the Description field in Compact Mode. To select **Compact Mode**, you must select **Full Mode** first to enable Compact Mode.

All included fields will appear in the Info Card. A field with neither **Full Mode** nor **Compact Mode** selected will not appear in the grid view but it will be available for the user to make visible.
 - c) To change the order in which the fields appear, drag the fields to a new location or change the sequence of numbers in the **Order** fields and click **Update Order**.
 - d) Specify whether each field is **Read-Only**.
 - e) To change the default column width for the fields, change the numbers in the **Column Width** fields.
 - f) To delineate a set of fields on the Info Card, click **Insert Section** and enter a name for the section heading. In the **Insert before** field, select the field that the section heading will appear before. If you have translated text for the section heading, add it to each language as required. Click **Apply**.

- g) Repeat these steps for each additional object type that you have included.
11. Click **Finish**.

Results

The grid view is added to the list of navigational views, where you can make it the default navigational view, have it appear higher in the list of navigational views, disable or enable it, or delete it.

Creating Activity Views

For each **Detail View** and **Activity View** for an object type within a profile, you can choose object fields and/or report fragment fields and set their order, insert section dividers, set fields to editable or read-only, and specify the number of columns each field will span (either one or two).

For **Activity Views**, you can also select up to three levels of object types, choose which paths to use to traverse the hierarchy for each level, select object-type filters to narrow the scope of returned search data, and determine the order of objects in a list or child hierarchy.

Before you begin: Activity view considerations

Before you create an Activity View, you need to determine the purpose of the view and identify the parent and child object types that will be included in the view. Planning your changes ahead of time helps to minimize the necessary work and prevents duplication of effort.

The following list will help you identify some of the questions you need to consider before you create a new Activity View:

- What task or activity does the user need to accomplish?
- What data does the user need displayed in this view to accomplish the task or activity?
- What are the object types that should be included in this view? Will levels be "skipped" in the object hierarchy?
- What field or fields does the user need to view or update?
- Are there constraints (such as a filter) that you need to put on the data in this view?
- If you plan to use a filter to remove extraneous objects that are not directly related to the current activity or to reduce the number of objects returned to a reasonable size, is the filter already configured for the selected object type? (For filter details, see [“Tasks to define filters for an object type” on page 267.](#))

Scenario

The following scenario describes how you might use the Activity View Wizard to create an Activity View called "Control Assessment by Risk Activity" for users who are "Control Assessors". Although the scenario does not include all the configuration features available in the Activity View Wizard, it does highlight many of the basic features.

Your organization created a profile called "Control Assessor" for users who have the responsibility to determine the effectiveness of controls.

To facilitate the work of a Control Assessor, you want to create a "Control Assessment by Risk Activity" view that would allow a Control Assessor to quickly analyze test results related to a particular control and then update the "Operating Effectiveness" field of a Control object accordingly.

In addition, you want the users to be able to perform their work with minimal navigation and provide only data relevant to accomplishing the task. If multiple test results are displayed, the data should be sorted according to the "Date Performed" field in ascending order.

To start, you would select the "Control Assessor" profile from the Profiles page and then select "SOXRisk" from the list of Object Types as this is the parent object type. You would then navigate to the Object View table and click the Add New icon to start the Activity View Wizard.

Table 129 on page 338 highlights the tasks you would perform on each screen in the Activity View Wizard to create a basic Activity View called "Control Assessment by Risk Activity". The table also includes a reference for each screen in the Wizard where you can find more details about that task.

<i>Table 129. Configuring a Sample "Control Assessment by Risk Activity" View</i>	
On this screen in the Activity View Wizard...	Do this...
1. Specify View Details (for details, see "Task 1: Specify view details" on page 341)	In the Name field, type the name: <i>Control Assessment by Risk Activity</i> . (For layout refer to pane "3" in Figure 19 on page 340.)
2. Select Object Types (for details, see "Task 2: Select object types" on page 341)	1. In the same row as Risk, click the Choose Object Types link and select Control. (For layout refer to panes "4" for Risk, and "5" and "6" for Control in Figure 19 on page 340.) 2. In the same row as Control, click the Choose Object Types link and select Test Result. (For layout refer to pane "7" in Figure 19 on page 340.) Note: Child object types can be at any level in the object hierarchy. In this example, we are "skipping" the Test object type between Control and Test Result.
3. Specify Object Type Settings (for details, see "Task 3: Specifying object type settings" on page 341)	In the same row as Test Result, click the Select Sort Criteria link and do the following: 1. Select the Date Performed field from the list. 2. Set the selected field to Ascending. (For layout refer to pane "7" in Figure 19 on page 340.)

Table 129. Configuring a Sample "Control Assessment by Risk Activity" View (continued)

On this screen in the Activity View Wizard...	Do this...
4. Specify Field Settings (for details, see “Task 4: Specify field settings” on page 342)	For each object type, click Choose Fields and select the following fields (if necessary, clear the Name field box as the name of the object is automatically displayed in the pane title). When finished with selecting fields, set the display order of each field as shown and click Update Order. • Risks (all Read-only fields. For layout refer to pane "4" in Figure 19 on page 340.) – 1 Description – 2 Inherent Risk Rating – 3 Category – 4 Subcategory • Control (mostly Read-only fields. For layout refer to pane "6" in Figure 19 on page 340.) – 1 Description – 2 Domain – 3 Control Type – 4 Control Method – 5 Design Effectiveness – 6 Operating Effectiveness (writable) • Test Result (all Read-only fields. For layout refer to pane "7" in Figure 19 on page 340.) – 1 Description – 2 Performed By – 3 Reviewed By – 4 Reviewer Conclusion – 5 Date Performed – 6 Test Result – 7 Exceptions – 8 Exception Description
5. Define Listing Columns (for details, see “Task 5: Define listing columns” on page 342)	Click Choose Fields and add the Description field to the listing pane for child Control objects. Click Finish when done. (For layout refer to pane "5" in Figure 19 on page 340.)

After the "Control Assessment by Risk Activity" view is saved, it becomes available as a selection in the **Current View** selection list on the Risk object detail page.

When a "Control Assessor" selects a particular risk for analysis and navigates to the detail page of that Risk object, that user can then click the **Current View** arrow and select the "Control Assessment by Risk Activity" view from the list of views.

When the "Control Assessment by Risk Activity" view is displayed on the page, the "Control Assessor" could then view the child controls and test results associated with that selected risk, discuss the test

results (sorted by Date Performed in ascending order), and then update the Operating Effectiveness field of that Control object accordingly.

The layout of Activity views

The layout of an Activity view page contains panes that are common to all views and panes that are unique to Activity views.

Figure 19 on page 340 shows the basic layout of an Activity view page.

The panes labeled "1" and "2" in Figure 19 on page 340 contain data common to all views, with pane "3" containing a combination of common and unique view elements.

The panes labeled "4" through "7" in Figure 19 on page 340 are unique to Activity Views. The pane labeled "4" contains the fields (configured in the Activity view wizard) for the top-level object. Pane "5" displays the list of first-level child objects for the selected top-level object. Data displayed in the listing pane is not editable.

When an object in the listing pane is selected, that object and its children are displayed in hierarchical panes (panes "6" and "7" in Figure 19 on page 340). Depending on the configuration, fields in the top-level object pane and in the hierarchical panes can be Read-only and/or editable.

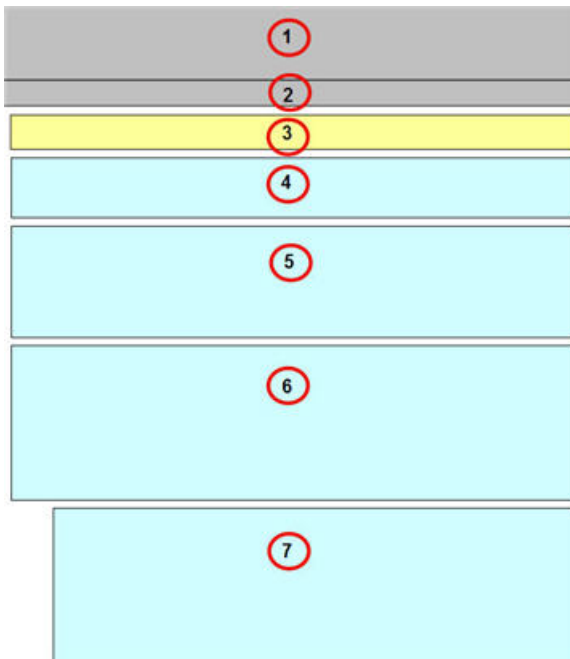


Figure 19. Layout of an Activity view page

The following numbered list describes the panes of an Activity view page as they are labeled in Figure 11.

1. Header pane - contains common elements such as a logo, logon user name, logout link, and the Reporting Period selector.
2. Menu bar - a common element used as the main navigation tool for accessing objects.
3. Navigation pane - contains breadcrumb links (common element) and the Current View selector, which is displayed when multiple Object Views are available.
4. Top-level Object Field pane - unique to Activity views - contains fields configured for the selected top-level object.
5. First-level Child Object Listing pane - unique to Activity views - contains a list of first-level child objects configured for the top-level object. If multiple first-level child object types are configured, a selector box is displayed that allows users to switch between object types.
6. Child Hierarchy pane for the selected first-level child object - unique to Activity views - contains fields configured for this object type.

7. Child Hierarchy pane for children of the selected child object - unique to Activity views - contains fields configured for this object type.

Task 1: Specify view details

The text you enter in the **Name** field for this view is also the initial label text for this view. If you want different label text to be displayed as the "name" of this Activity or Grid view to application users for selection in Current View selection list, make sure to enter text in the appropriate language translation field.

Procedure

1. In the **Name** field, type a name for this Activity or Grid View.
2. Click the **Translate** link and type the label text you want to be displayed to users in the appropriate language field, and then click **Apply**.

Note: If you do not enter translated label text for the **Name** field, the text you entered in Step 1 will be displayed to application users in the Current View selection list.

3. Click **Next**.

Task 2: Select object types

Activity or Grid views will display up to three levels of objects (the top-level object, list and detail panes for child objects, and objects under a selected child object). You can choose child object types at any level in the hierarchy for display in an Activity view.

Procedure

1. In the **Actions** column, click the **Choose Object Types** link in the row containing the selected object type (for example, RiskAssessment) to which you want to add child objects.
2. In the **Choose Object Types** box, select the box next to each child object type you want to display (for example, Risk) under that object type. When finished, click **Apply**.
3. Optional: Click the **Choose Object Types** link next to an associated object type (from Step 2), and select any object types you want to display (for example, Control) under that object type. When finished, click **Apply**.
4. Click **Next**.

Task 3: Specifying object type settings

A path is a specific branch of objects through the hierarchy. For associated objects that have multiple paths, you can choose which object paths to use to return data for that object type.

When a single path exists between one object level and the next, you do not have to select a path. Paths that loop back to the top-level object type are excluded from the selection list.

Procedure

1. For associated objects that have multiple paths, complete the following steps to specify the paths to use through the object hierarchy to retrieve data:
 - a) Click the **Choose Paths** link under the **Actions** column in the row that contains the object type in Task 1 (if necessary, scroll down the page to see it).
 - b) In the **Choose Paths** box, select or clear the box next to each object path that you want the application to use or ignore for retrieving associated object data.
 - c) Click **Apply**.

The selected paths are listed in the **Paths** column.

Note: Descendants of recursive object types, such as Business Entity, appear under all of their ancestors, not just the most immediate ancestor. For example, if the path is set to Business Entity/Preference and the hierarchy of objects is North America Division/US Region/Pref1, Pref1 appears as a descendant of both North America Division and for US Region.

2. To specify how objects types are sorted in a listing or child hierarchy pane, click the **Select Sort Criteria** link under the **Actions** column in the row of the object type that you want.

3. In the **Specify Sort Criteria** field, complete the following steps:

- a) In the **Available Fields** pane, select each object field to use for sorting.

Note: A sort field does not have to be displayed to in order to use the field for sorting a list or child hierarchy pane.

- b) Click the double arrows to move object fields forward (>>) or backwards (<<) between the **Available Fields** and the **Selected Fields** panes.

- c) In the **Selected Fields** pane, select a sort field and click any of the following icons:

Table 130. Sort icons	
Click this icon...	If you want to...
▲ (triangle up)	Sort objects in ascending order. This value is the default setting.
▼ (triangle down)	Sort objects in descending order.
⬆ (up arrow)	Move up the field in the list.
⬇ (down arrow)	Move the field down in the list.

- d) Click **Apply**.

4. To specify a filter for an object type, click **Choose Filter** in the **Actions** column that corresponds to the object type

5. In the **Choose Filter** field, select the filter to use and click **Apply**.

6. Click **Next**.

Task 4: Specify field settings

You can choose the fields you want displayed in top-level and child hierarchy panes.

Fields can be object fields, computed fields, and report fragment fields.

Procedure

1. To specify the display fields for an object type, click **Choose Fields** under the object type.
 - a) In the **Choose Fields** selection box, select the box next to each field you want to include.
 - b) When finished, click **Apply**.
2. Optional: Insert a section. For details, see [“Inserting section headings” on page 346](#).
3. Optional: Change the display order of the fields. For details, see [“Setting the display order of fields in a view” on page 329](#).
4. Click **Next**.

Task 5: Define listing columns

You can choose the fields you want displayed for table columns in a first-level child listing pane.

Procedure

1. To specify the table columns for the pane in which associated objects are listed:

- a) In the **Choose Fields** selection box, select the box next to each object field you want to include as a table column. By default, the **Name** field is selected.
- b) When finished, click **Apply**.
2. Optional: Change the display order of the fields. For details, see [“Setting the display order of fields in a view”](#) on page 329.
3. Click **Finish**.

Modifying an Activity view

When you modify an **Activity view**, you use the Activity view wizard to make the required changes. Each step in the wizard becomes an active link so you can go directly to that step and make the required changes.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type (for example, RiskAssessment) you want to modify.
4. From the **Object Views** table listing, click the name of an Activity View you want to modify to open the Activity View wizard.
5. Click a link in the wizard that corresponds with the type of change you want to make. Refer to [“Creating Activity Views”](#) on page 337 for an overview of tasks.
6. Click **Save**.

Creating a Creation view

In IBM OpenPages with Watson, you can create a creation view.

About this task

You can use Creation views to create multiple Add New view definitions for a single object type for a single profile.

Procedure

1. Click **Administration > Profiles** and select a profile.
2. Select the object that will be at the root of the creation view.
3. From the menu bar, click **Creation Views**.
4. In the **Creation Views** section, click **Add New**.
5. To provide details about the new creation view, complete the following actions:
 - a) Add a name and description. Optionally, enter the translations for the name. The description is for administrators only.
 - b) If the creation view is not ready for users to access now, clear the **Enabled** check box. The new creation view is enabled by default.
 - c) Click **Next**.
6. To select the child objects to associate with the current object, complete the following actions:
 - a) Under **Actions**, click **Choose Object Types**.
 - b) Select the object types to associate.
Only direct child objects are available to associate.
 - c) Click **Apply**.
 - d) Click **Next**.

7. Choose the objects that you want show on separate pages in the Add New wizard: check box
 - a) For each object that you want to show on its own tab, select the **Separate page** check box.
By default, any objects that do not have a separate page are shown together on the Associate tab.
 - b) Click **Next**.
8. To configure fields for the creation view, complete the following actions:
 - a) To select the fields that will be shown, click **Choose Fields**, select the fields, and click **Apply**.
 - b) To change the order in which the fields are shown, change the sequence of numbers in the **Order** fields and click **Update Order**.
 - c) Specify whether each field is **Read-Only**.
 - d) To specify a name for the object-specific tab, click **Insert Page** and enter a name for the section heading.
By default, the tab name is the Properties tab.
9. Click **Finish**.

Configuring fields in Detail and Activity views

For each **Detail** and **Activity** view that you configure for an object type within a profile, you can select which fields you want to include or exclude in that view.

Fields can be object fields, computed fields, and report fragment fields.

When you include fields in a Detail or particular Activity view, the additional fields are immediately visible to all users and are displayed in table rows on that view page.

For **Detail** views, only the object fields that you configure are used by the **Export** function (in .xls format) on a **Filtered List View** page (report fragment fields are ignored).

Each object type has a set of predefined object fields that consist of both shared and object-specific fields. The shared object fields (such as *Name*, *Description*, *Created By*, and so forth) are common to all object types and belong to the System Field field group. With the exception of the **Name** field, which is required and always in position 1, you can choose which system and object-specific fields to include or exclude from an object view. In this way, you can tailor each view to accommodate changing business needs

Including fields in Detail and Activity views

Before you include a field in a Detail or Activity view, the field must be visible in the object field list.

Fields can be object fields, computed fields, and report fragment fields.

If the field is part of a field group, make sure you include the field group for the object type. For more information, see [“Including field groups for an object type \(Standard UI\)” on page 255](#).

Note: When dependent fields are included in a Detail or Activity view, make sure to include both the controlling field and required dependent fields. If the controlling field that requires that a user enter a value in a dependent field is included in a view and the required dependent field is excluded, the user cannot complete the operation. The following error message will be displayed, "A field not available to you has been made required by a field dependency so you will be unable to continue with this operation."

When you include object fields in a Detail or Activity view for the selected object type, the object fields are displayed as table rows in that view.

Although you cannot modify the parameters of the table, you can set a field to span table columns.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.

3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. From the **Object Views** tab listing, select the view you want:

Table 131. Object views	
For this type of view...	Do this...
Detail View	Click the Detail link.
Activity View	a. Click the name of the Activity view you want. b. In the Activity View wizard, click the Specify Field Settings link.

5. To add fields to an object type:
 - a) Click **Choose Fields** for the object type you want.
 - b) In the **Choose Fields** selection box, select the box next to each field you want to include.
 - c) Click **Apply** or **Save**.
6. To modify the order in which the fields are displayed in the table rows on a Detail or Activity view, see [“Setting the display order of fields in a view”](#) on page 329.
7. To format the field so it spans table columns, see [“Spanning table columns”](#) on page 347.

Excluding fields from Detail and Activity views

When you exclude fields from a Detail or Activity view for the selected object type, the fields are removed from the table rows on that view page.

Fields can be object fields, computed fields, and report fragment fields.

With the exception of the **Name** field, you can exclude any field from an object view. For example, if you exclude the **Description** field from a Filtered List view for an object type, field is dynamically removed from the Filtered List view page and the change is immediately visible to users.

Note: If you exclude object fields that are referenced by JSP reports, the report may fail or return unexpected results.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. From the **Object Views** tab listing, select the view you want:

Table 132. Object views	
For this type of view...	Do this...
Detail View	Click the Detail link.
Activity View	a. Click the name of the Activity view you want. b. In the Activity View wizard, click the Specify Field Settings link.

5. To remove fields from an object type:
 - a) Click **Choose Fields** for the object type you want.
 - b) In the **Choose Fields** selection field, clear each field to remove from this view.

- c) Click **Apply** or **Save**.

Inserting section headings

Section headings are an optional formatting feature. Use section headings to delineate a set of fields on a page. Before you create a section heading, identify where to insert it on a Detail or Activity view page. A section heading is displayed on the page before whichever field you specify.

Fields can be object fields, computed fields, and report fragment fields.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. For the **Detail** view, click the **Detail** field.
4. For an **Activity** view, click the name of the Activity view and click **Specify Field Settings**.
5. To insert a section heading in the selected view:
 - a) Select **Insert Section** for the object type.
 - b) In the **Section Information** pane, provide the following information:

Table 133. Section information fields	
Field	Action
Name	Required. Type a name for the section heading.
Insert before field	Select a field from the list. The section heading is displayed before the selected field.
language-specific (for example, Japanese)	Type a text string to use as the translated display text label for the section heading. If no translation text is entered, the entry in the Name field is displayed.

6. Click **Apply** or **Save**.

Modifying section headings

Section headings are an optional formatting feature. You can use section headings to delineate a set of fields on a page. After you create a section heading, you can modify the label text used for translation.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. From the **Object Views** table listing:
 - For the **Detail** view - click the **Detail** link.
 - For an **Activity** view:
 - a. Click the name of the Activity view you want.
 - b. In the Activity View wizard, click the **Specify Field Settings** link.
5. To modify a section heading in the selected view:
 - a) Click **Insert Section** for the object type you want.

- b) On the object type tab, click the **Edit** link under the **Actions** column in the row containing the section that you want to modify.
- c) In the **Section Information** box, make the changes as wanted.
- d) Click **Apply** or **Save** to effect the change.

Deleting section headings

Section headings are an optional formatting feature. You can use section headings to delineate a set of fields on a page. You can remove section heading. After a section is deleted, it is permanently removed and cannot be restored.

Procedure

1. Click **Administration > Profiles**
2. Select the profile to modify.
3. From the **Object Types** listing, click the name of the object type to modify.
4. In the **Object Views** pane, click the Detail link or the Activity view to modify.
5. To delete the section in the Detail view, click **Delete** next to the section to delete.
6. To delete a section in an Activity view, click the **Specify Field Settings** link. Then, click **Delete** next to the section to delete.

Setting object fields as read-only or editable

You can configure object fields on an Object View page within a profile to be view only or editable to users assigned that profile by either selecting or clearing the **Read-Only** box for a field.

Note: Report fragment fields, computed fields, and certain system fields (such as "Last Modified By", "Created By", "Creation Date" and so forth) are set, by default, to Read-Only and cannot be changed.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. Select a Views tab, and click the name of the view link you want to modify (for example, *Detail*) to open its detail page.
5. On the edit page for the selected object type, do the following in the row for each object field you want to modify:
 - To make a field non-editable - select the **Read-Only** box.
 - To make a field editable - clear the **Read-Only** box.
6. Click **Save**.

Spanning table columns

In **Detail Views**, **Activity Views**, and **Context Views**, fields are typically displayed on the page in rows within a two-column table format. You can make a row containing a field span table columns by configuring the **Span Columns** setting.

Note:

- For object fields with a Text Area display type, you can configure the text box size by setting the number of rows and columns. By default, the rows are set to 5, and the columns are set to 60.

- For report fragment fields with an Automatic display type, you can configure the cell height of the report element. By default, this is set to 235 pixels.

The **Span Columns** setting is displayed for all field display types and the process of setting it is the same.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type containing the object field you want to modify (for example, SOXControl).
4. On the **Object Fields** table for the selected object, click the name of the field to open its detail page (for example, *Who Performs Control?*).
5. On the **Display Type Information** table, click **Edit**.
6. On the edit page, click the Span Columns arrow and select a value from the list:
 - Select **False** if you want the row containing the field to be displayed within a table column and not span the columns of the table.
 - Select **True** if you want the row containing the field to span the columns of the table.
7. Click **Save**.

Configuring the display type for reporting fragment fields (Standard UI)

You can configure how reporting fragment fields are displayed to application users on Detail and Activity View pages. Reporting fragment fields are always read-only fields.

Reporting fragment fields can be displayed as follows:

- **Automatic** - this setting embeds the report element directly into the cell for the field and displays it as a view-only field on the page.

You can also configure the cell height of the field. By default, it is set to 235 pixels.

- **On Demand** - this setting displays a clickable icon  in the field that opens the report element in a pop-up window. For information on automatically sizing pop-up windows, see [“Report fragment settings”](#) on page 612.

Note: Changing the display type setting will affect the display of this field in all profiles.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type containing the report fragment field you want to modify (for example, SOXControl).
4. On the **Object Fields** table for the selected object type, click the name of a report fragment field to open its detail page.
5. On the **Object Field Information** table:
 - a) Click **Edit**.
 - b) On the edit page, click the **Display Type** arrow and select a value from the list.
 - c) Click **Save**.
6. Optional: For Automatic display types only. If the display type is On Demand, skip this step. You can modify the cell height of the report fragment field:

- a) On the **Display Type Information** table, click **Edit**.
 - b) On the edit page, modify the number of pixels in the **Cell Height** box.
 - c) Click **Save**.
7. To make the row with the report fragment field span table columns, see [“Spanning table columns” on page 347](#).

Configuring display types for simple string fields (Standard UI)

For object fields that have a Simple String data type, you can configure how string data displays to users on an object’s details page. The display types for Simple String data fall into two basic categories: selector types for displaying users and/or groups, and text area display types for displaying text and URL information.

Note: Changing the display type setting affects the display of this field in all profiles.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type containing the object field you want to modify (for example, SOXControl).
4. On the **Object Fields** table for the selected object type, click the name of the object field to open its detail page.
5. On the **Object Field Information** table, click **Edit**.
6. On the edit page:
 - a) To make the field required, select the **Required** box.
 - b) To select a different display type, click the **Display Type** arrow and select a value from the list:
 - For user or group selector display types, see [“Configure user and group selectors display types for simple strings \(Standard UI\)” on page 353](#).
 - For a Business Entity Selector display type, see [Configuring the Business Entity Selector display type for simple string fields](#).
 - For a rich text display type, see [“Configuring rich text display types for simple strings \(Standard UI\)” on page 349](#).
 - For a box and URL display types, see [“Configuring text and URL display types for simple strings \(Standard UI\)” on page 351](#).
 - For a plain text area display type, see [“Configuring text area display types for simple strings \(Standard UI\)” on page 353](#).
7. To have a row with a field span table columns, see [“Spanning table columns” on page 347](#).
8. Click **Save**.
9. If you set the display type of a field to Multi-Valued User Selector or Multi-Valued Group Selector or Multi-Valued User Group Selector, update the reporting schema. For more information, see [“Updating the reporting schema” on page 162](#).

Results

Note: To change a field to **Read-Only**, see [“Setting object fields as read-only or editable” on page 347](#).

Configuring rich text display types for simple strings (Standard UI)

The rich text display type provides a text display area with a toolbar and commands for text formatting and word processing. The toolbar can be minimized or expanded.

When this feature is used, you may not be able to enter 4000 rich text characters into the text display area because of the space used for formatting and multi-byte characters.

Note: When generating reports in PDF format, rich text fields do not render properly and the format is not preserved.

To modify these settings, click **Edit** on the **Display Type Information** tab.

You can configure the size of the display area with the following settings:

Table 134. Rich text display settings	
Setting	Description
Rows	The display length of the area, which includes the rich text editor interface and text input area. The default value is 250 rows. To change the value, type a number in the box.
Row Units (pixels or percent)	The unit of measure in pixels or percent for the Rows setting. The default value is "Percent". To change the value to "Pixels", select the Pixels icon.
Columns	The percent or number of pixels allocated to the width of the display area, which includes the rich text editor interface and text input area. The default value is 100 percent. To change the value, type a number in the box. To change the unit of measure, use the Column units setting.
Column units	The unit of measure in pixels or percent for the Columns setting. The default value is "Percent". To change the value to "Pixels", select the Pixels icon.

For instructions on how to configure a display type for a string data type object field, see [“Configuring display types for simple string fields \(Standard UI\)”](#) on page 349.

Configuring the Business Entity Selector display type for simple string fields (Standard UI)

For the Business Entity Selector display type, you can select a starting business entity, establish the number of levels that users can navigate, and determine whether to span columns.

To modify these settings, click **Edit** on the **Display Type Information** tab.

You can configure the following settings:

Table 135. Business Entity Selector display settings	
Setting	Description
Starting Business Entity	Click the icon beside the Starting Business Entity box, and use the Recently Used , Browse or Search tabs to select a starting business entity. Type a term in the Search field to find an exact match to the object name or description. Note: Optionally, if you want all Level 1 business entities displayed, enter a forward slash (/) in the Search box. If you leave this field blank, it will default to a slash when you save.

Table 135. Business Entity Selector display settings (continued)	
Setting	Description
Number of Levels	Determines the number of levels that end users can navigate to from the starting business entity. For example, if you select Global Financial Services as your starting business entity and set the number of levels to 2, you can navigate to two levels below Global Financial Services (Global Financial Services/Asia Pac/Agency Services). Limit the number of levels to improve performance of the selector and help users select from the entities most appropriate for this field. The default value is 3.
Span Columns	Determines whether to make a row span columns. The default value is false. This setting will be ignored by views that do not support column spanning. For more information, see Spanning table columns

For instructions on how to configure a display type for a simple string data type object field, see “Configuring display types for simple string fields (Standard UI)” on page 349.

Known issue

A known issue exists when values in business entity selector fields are updated in the following scenario. A user in the OpenPages application chooses a business entity for a business entity selector field and saves it. The entity folder is correctly inserted in the business entity selector field. If the user then clicks **Action > Edit this Business Entity** and changes the name of the business entity, the value in the business entity selector field is not updated with the new name. If the user clicks **Action > Edit this Business Entity** again and selects the icon next to the business entity selector field, the select entity is now empty.

Configuring text and URL display types for simple strings (Standard UI)

The text and URL display types provide a box area in which users can enter a string value. For these display types, you can control the length of the display box and the number of characters users can enter for a string value.

Note: The URL display type validates that the internet address is a fully-qualified URL internet address (for example, <http://www.mycompany.com> or <ftp://ftp.myftpsite.com>) and will display an error message to the user if the format of the internet address is incorrect.

To modify these settings, click **Edit** on the **Display Type Information** tab.

For text and URL display types, you can configure the following settings:

Table 136. Text and URL display settings	
Setting	Description
Columns	The display length of the box area. The default value is 30. To change the value, type a number in the box.
Maximum Length	The maximum number of bytes allowed to be entered for a string value. The default value is 4000. To change the value, type a number in the box.

For instructions on how to configure a display type for a string data type object field, see “[Configuring display types for simple string fields \(Standard UI\)](#)” on page 349.

An alternative to using the URL display type is to use the rich text display type to display a user-friendly link name. For information, see “[Configuring URL link names by using the rich text display type for simple strings \(Standard UI\)](#)” on page 352.

Configuring URL link names by using the rich text display type for simple strings (Standard UI)

You can use the rich text display type to display a user-friendly link name as a field's default value. For example, you can configure a field's default value to display as **My Company** rather than **http://www.mycompany.com**. This feature is an alternative to using the URL display type, which can display only URL internet addresses.

About this task

When you use the rich text display type, you can define the URL by using the anchor tag, `<a>`. The anchor tag specifies the link name and styles you want to apply, such as font style and size. The `target="_blank"` tag makes the URL open in a new tab.

For example, the following anchor tag displays the link name, **My Company**, and opens `http://www.mycompany.com` in a new tab:

```
<a href=" http://www.mycompany.com" target="_blank">My Company</a>
```

The following anchor tag applies a larger font and different color to the link name:

```
<a style="font-size:18px;font-family:comic sans ms,cursive;color:#FF0000" href=" http://www.mycompany.com" target="_blank">My Company</a>
```

You can put multiple anchor tags in a single rich text field. For example, the follow anchor tags display two link names as a field's default value:

```
<a href=" https://www.ibm.com" target="_blank">Link to IBM</a>  
<a href=" https://www.ibm.com/docs/en/opw" target="_blank">Link to IBM Documentation</a>
```

Because you are using the rich text display type rather than the URL display type, the system does not check whether the URL is valid.

You can add fields that use the rich text display type for link names to all view types. However, on Filtered List and Grid views the link name is displayed above a glasses icon. Clicking the icon opens a window that contains the link.

Procedure

1. Click **Administration > Field Groups**.
2. Select a field group.
3. In the **Field Definitions** table of the field group, click **Add**.
 - a) In **Data Type**, select Simple String.
 - b) Click the double arrows (**>>**).
 - c) In **Default Value**, enter the URL address as an anchor tag, for example:

```
<a href=" http://www.mycompany.com" target="_blank">My Company</a>
```

4. Click **Administration > Profiles**.
 - a) Select a profile.
 - b) Select an object type.

- c) Click **Include** and choose the new field.
 - d) Click the field in the **Object Fields** table and click **Edit**.
 - e) In **Display Type**, select Rich Text.
5. Add the field to a view. Select **Read Only**.

What to do next

Create objects and use the new field. Since the URL is specified as a default value, the field does not display on existing object instances.

Configuring text area display types for simple strings (Standard UI)

The text area display type provides a box display area in which users can enter either plain or HTML-formatted text.

To modify these settings, click **Edit** on the **Display Type Information** tab.

You can configure the size of the display area with the following settings:

Table 137. Text area display settings	
Setting	Description
Rows	The display length of the box area. The default value is 5 rows. To change the value, type a number in the box.
Columns	The display width of the box area. The default value is 60. To change the value, type a number in the box.

For instructions on how to configure a display type for a simple string data type object field, see [“Configuring display types for simple string fields \(Standard UI\)”](#) on page 349.

Configure user and group selectors display types for simple strings (Standard UI)

You can configure a user, group, user/group, multi-valued user, multi-valued group, or multi-valued user/group selector display type for a simple string data type object field. An object field that has a selector display type allows an application user to click either an arrow  and select user names from a drop-down list box or a magnifying glass icon  and search for users or groups from a pop-up dialog box.

Object fields with a display type of user selector or multi-valued user selector accept only user names as valid values. For example, Control Owner is an object field for the control object.

The following selector display types are available for simple string data types:

Table 138. User and group display settings	
Selector Display Type	Description
User Dropdown	On Detail and Activity views provides an arrow  that users can click to display a drop-down list box of user names. On all other views provides a magnifying glass icon  that users can click to display a search pop-up dialog box to search for a user.

Table 138. User and group display settings (continued)

Selector Display Type	Description
User Selector	Provides a magnifying glass icon  that users can click to display a search pop-up dialog box to search for a user.
Group Selector	Provides a magnifying glass icon  that users can click to display a search pop-up dialog box to search for a group.
User/Group Selector	Provides a magnifying glass icon  that users can click to display a search pop-up dialog box to search for a user or group.
Multi-Valued User Selector	Provides a magnifying glass icon  that users can click to display a search pop-up dialog box to search for multiple users.
Multi-Valued Group Selector	Provides a magnifying glass icon  that users can click to display a search pop-up dialog box to search for multiple groups.
Multi-Valued User/Group Selector	Provides a magnifying glass icon  that users can click to display a search pop-up dialog box to search for multiple users or multiple groups.

Depending on the selector display type, you can configure some or all of the following settings.

To modify these settings, click **Edit** on the **Display Type Information** tab.

Note: These settings are also applied to the User and Group Search function.

Table 139. Additional selector display type settings

Setting	Description
Include Disabled	Allows or disallows disabled user accounts to be included in a selector listing. If the Include Disabled value is set to: • True - disabled user accounts are included in the selector listing. When this setting is selected, the Minimum Access setting is disabled. A value of True, when used in combination with a Starting Group value that contains many users, can result in slower search performance. • False - disabled user accounts are excluded from the selector listing. When this setting is selected, the Minimum Access setting is enabled. This setting generally applies to User (not Group) selectors. Note: There is a known issue with the Include Disabled setting. If the Display Type is User Dropdown, Include Disabled is set to True, and disabled users exist and should be listed, the disabled users are not listed and instead the message <code>No items to display</code> is shown.

Table 139. Additional selector display type settings (continued)

Setting	Description
Starting Group	Controls which group displays at the beginning of the selection hierarchy. If the Starting Group value is blank, selectors search the system for all users and/or groups, depending on the display type. A blank Starting Group value used in combination with an Include Disabled value of True can result in improved search performance. To select a starting group, click the group icon and select a valid group name from the selector window. For example, if you are using role-based security, you could select the Security Domains group, for non role-based security, you could select the Workflow, Reporting and Others group. Note: There is a known issue with the Starting Group setting. In the Add New wizard, the Starting Group setting is not applied to fields that have Display Type set to User dropdown.
Include Subgroups	Controls whether subgroups are included or excluded from the User selector listing. Note: This setting applies only to the User/Group and Group selectors. If the Include Subgroups value is set to: • True - subgroups are included in the selector listing. • False - subgroups are excluded from the selector listing.

Table 139. Additional selector display type settings (continued)

Setting	Description
Minimum Access • Read • Write • Delete • Associate	This setting is enabled only if the Include Disabled value is set to False. This setting allows you to filter users based on access control list settings on an object's folder. For example, you want to limit the number of users who can be assigned as a Process "Cycle Owner", which is an object field with a user selector display type for the Process object. Because you previously set up an access control list (ACL) for one or more groups or users to the Process folder, you can use the Minimum Access setting to filter the list of users. If you only wanted users with "Delete" permissions to be displayed on the user selector list, you can select the "Delete" Minimum Access setting to filter and display only those users with "Delete" ACL permissions. If the Read box is: • Selected - only users with Read access are displayed on the user list. • Cleared - no filtering occurs. If the Write box is: • Selected - only users with Write access are displayed on the user list. • Cleared - no filtering occurs. If the Delete box is: • Selected - only users with Delete access are displayed on the user list. • Cleared - no filtering occurs. If the Associate box is: • Selected - only users with Associate access are displayed on the user list. • Cleared - no filtering occurs.

Changing the display type



Attention:

If you change the display type of the actor fields in the profiles, you must take action on the filters.

Table 140. Display type changes that require action

If you change this display type	To this display type	Take this action ¹
User Selector	Group Selector or Multi-Valued Group Selector	A
	User/Group Selector or Multi-Valued User/Group Selector	B
User Dropdown	Group Selector or Multi-Valued Group Selector	A
	User/Group Selector or Multi-Valued User/Group Selector	B

<i>Table 140. Display type changes that require action (continued)</i>		
If you change this display type	To this display type	Take this action¹
User/Group Selector	Group Selector or Multi-Valued Group Selector	A
	User/Group Selector or Multi-Valued User/Group Selector	B
Group Selector	Multi-Valued Group Selector	A
	User/Group Selector or Multi-Valued User/Group Selector	B
Multi-Valued User Selector	Multi-Valued Group Selector	A
	Multi-Valued User/Group Selector	B
Multi-Valued Group Selector	Multi-Valued User/Group Selector	A
Multi-Valued User/Group Selector	Multi-Valued Group Selector	A

¹Actions

- A: If you make this change, and if "End User" is set as the filter value for that actor field in the filter, the "End User" must be updated to the group so that the filters can return the expected results.
- B: If you make this change, re-save the filter so that it can return the expected results.

If you set or change the display type of a field to Multi-Valued User Selector or Multi-Valued Group Selector or Multi-Valued User Group Selector, update the reporting schema. For more information, see [“Updating the reporting schema” on page 162](#).

You cannot change a Multi-Valued User Selector, Multi-Valued Group Selector, or Multi-Valued User/Group Selector display type to a single actor display type.

Controlling user selector performance

If your deployment has a large number of users, the performance of the User Selector or the Multi-Valued User Selector in opening and loading data may be sluggish. One way to improve the performance of the User Selector or the Multi-Valued User Selector is to configure it so it only retrieves users that have permission on the object being edited.

The supplied profiles in the IBM OpenPages with Watson application are configured such that the User Selector or Multi-Valued User Selector pop-up will retrieve all users in the system - including some application users who do not have security permissions on the selected object. This may result in the assignment of a user as "owner" on an object when the user does not have read access on the object.

The following steps explain how to restrict the set of users retrieved by the User Selector or the Multi-Valued User Selector to those users that have access permissions on the object being edited at the time.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type containing the object field you want to modify (for example, SOXControl).
4. On the **Object Fields** table for the selected object, click the name of the object field with the User Selector display type to open its detail page (for example, Control Owner).

5. On the **Display Type Information** tab, click **Edit**.
6. On the edit page:
 - a) Under **Minimum Access**, select the **Read** box. This will restrict the users that are displayed in the User Selector to the set of users that have read permission on the object.
 - b) Optionally, select other permissions to further restrict the users that are available in the User Selector based on the users' permissions.
7. Click **Save**.

Modifying user and group selectors

On a small number of administrator screens, for example, **Administration > Object types > Add Filter** or **Edit Filter**, the pop-up dialog box for the User and Multi-Valued User Selectors displays user names in a phonebook style, and you can configure the number of users per category within the phonebook. Groups appear in a hierarchical tree style.

You can also configure the selector display types to open a search box instead of a phonebook style box. For more information, see [“Actor selectors: Configure users and group selectors for search” on page 607](#).

For all the selector display types, you can configure additional display information for users, such as the user's e-mail address or first or last name.

Modifying the phonebook

The User Selector and Multi-Valued User Selector display user names in a phonebook style pop-up dialog box. User names within the phonebook are grouped into data buckets.

Each data bucket has the following characteristics:

- The names of the first and last users in a given bucket are used to show the scope of the bucket.
- The user names in a bucket can be expanded by clicking the plus sign, or collapsed by clicking the minus sign.
- The size of a bucket can be configured through the **Bucket Size** setting. For configuration details see, [“Actor selectors: Configure the bucket size of the phonebook” on page 605](#).

Modifying the selector dialog box

You can show additional information (such as a user's email address, first name, and last name) in the pop-up dialog box used for selecting users and groups.

You can add one or more additional columns by configuring the **Display** setting. For configuration details see, [“Actor selectors: Configure display columns in a selector dialog box” on page 606](#).

By default, only the **Name** and **Description** columns are displayed in this selection box. You cannot change or remove the **Name** column - it is always the first column and contains the Username of a user or group.

You can also change the format of the bucket heading for a locale. For configuration details see, [“Modifying the bucket heading format of the phonebook” on page 567](#).

Configuring display types for long string fields (Standard UI)

For object fields that have a long string data type, you can configure how long string data displays to users on an object's details page.

There are two subtypes of long text fields: medium and large. The size of medium long text fields is fixed to 32KB. The size of the large long text fields is set by default to 256000 bytes, but that can be increased by changing the **Platform > Repository > Resource > Large Text > Maximum Size** setting.

Be aware of the space used for non-printing characters (such as tabs and line breaks), and formatting and multi-byte characters (Rich Text display types). These may cause the data to exceed the size of the long string field, resulting in a message such as:

OP-03381: The specified value for "MyMediumLong" is too long. The 32966 characters entered (32966 bytes) exceeds the maximum size of 32768 bytes. Reduce the number of characters and re-enter the text. Note that character count includes non-printing characters, such as spaces, tabs, and line breaks.

The display types for medium long string data are: On Demand, On Demand Rich Text, Text Area, and Rich Text. The On Demand Rich Text display type is available only in the Standard UI.

The display types for large long string data are: On Demand and On Demand Rich Text. The On Demand Rich Text display type is available only in the Standard UI.

Both medium and large long string fields default to the On Demand display type.

Note: Changing the display type setting will affect the display of this field in all profiles.

For more information on long text fields, see [“Data types” on page 203](#).

Procedure

1. Access the **Profiles** page (see [“Accessing profiles” on page 298](#)).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type containing the object field you want to modify (for example, SOXControl).
4. On the **Object Fields** table for the selected object type, click the name of the object field to open its detail page.
5. On the **Object Field Information** table, click **Edit**.
6. On the edit page select the **Required** box to make the field required.
7. Click the **Display Type** arrow and select a value from the list to select a different display type:
 - For On Demand and On Demand Rich Text, see [“Configuring the on demand display types for long string fields \(Standard UI\)” on page 359](#). This applies to both medium and large long string fields.
 - For a Text display type, see [“Configuring text display types for medium long string fields \(Standard UI\)” on page 360](#). This applies only to medium long string fields.
 - For a Rich Text display type, see [“Configuring rich text display types for medium long string fields \(Standard UI\)” on page 360](#). This applies only to medium long string fields.
8. Click **Save**.

Note: To change a field to **Read-Only**, see [“Setting object fields as read-only or editable” on page 347](#).

Configuring the on demand display types for long string fields (Standard UI)

You can configure how long string fields are displayed on demand and on demand rich text to application users on Detail and Activity View pages.

Long string fields can be displayed as on demand and on demand rich text. Both settings allow users to edit the field in a pop-up window. On demand displays text. On demand rich text displays the data in rich text format.

The On Demand Rich Text display type is available only in the Standard UI.

The on demand rich text display type provides a text display area with a toolbar and commands for text formatting and word processing. The toolbar can be minimized or expanded. When this feature is used, be aware of the space used for non-printing, formatting, and multi-byte characters. These may cause the data to exceed the size of the long string field, resulting in a message such as:

OP-03381: The specified value for "MyMediumLong" is too long. The 32966 characters entered (32966 bytes) exceeds the maximum size of 32768 bytes. Reduce the number of characters and re-enter the text. Note that character count includes non-printing characters, such as spaces, tabs, and line breaks.

Note:

- When generating reports in PDF format, rich text fields do not render properly and the format is not preserved.
- Changing the display type setting will affect the display of this field in all profiles.

In **Detail Views** and **Activity Views**, fields are typically displayed on the page in rows within a two-column table format. To make the row containing the field span the table columns, see ["Spanning table columns"](#) on page 347.

Configuring text display types for medium long string fields (Standard UI)

The Text display type provide a box area in which users can enter a medium long string value. For these display types, you can control the length of the display box and the number of characters users can enter for a string value.

Note: This only applies to medium long string fields.

To modify these settings, click **Edit** on the **Display Type Information** tab.

For the Text display type, you can configure the following settings:

Table 141. Text display settings	
Setting	Description
Rows	The display length of the box area. The default value is 25 rows. To change the value, type a number in the box.
Columns	The display width of the box area. The default value is 60. To change the value, type a number in the box.
Span Columns	In Detail Views and Activity Views , fields are typically displayed on the page in rows within a two-column table format. You can make a row containing a field span table columns by configuring the Span Columns setting. The default is true. When true, the row containing the field will span the columns of the table. When false, the row containing the field will be displayed within a table column and not span the columns of the table.

For instructions on how to configure a display type for a string data type object field, see ["Configuring display types for long string fields \(Standard UI\)"](#) on page 358.

Configuring rich text display types for medium long string fields (Standard UI)

The rich text display type provides a text display area with a toolbar and commands for text formatting and word processing. The toolbar can be minimized or expanded.

When this feature is used, be aware of the space used for non-printing, formatting, and multi-byte characters. These may cause the data to exceed the size of the medium long string field, resulting in a message such as:

OP-03381: The specified value for "MyMediumLong" is too long. The 32966 characters entered (32966 bytes) exceeds the maximum size of 32768 bytes. Reduce the number of characters and re-enter the text. Note that character count includes non-printing characters, such as spaces, tabs, and line breaks.

Note: When generating reports in PDF format, rich text fields do not render properly and the format is not preserved.

To modify these settings, click **Edit** on the **Display Type Information** tab.

You can configure the size of the display area with the following settings:

Table 142. Rich text display settings	
Setting	Description
Rows	The display length of the area, which includes the rich text editor interface and text input area. The default value is 250 rows. To change the value, type a number in the box.
Row Units (pixels or percent)	The unit of measure in pixels or percent for the Rows setting. The default value is "Percent". To change the value to "Pixels", select the Pixels icon.
Columns	The percent or number of pixels allocated to the width of the display area, which includes the rich text editor interface and text input area. The default value is 100 percent. To change the value, type a number in the box. To change the unit of measure, use the Column units setting.
Column units	The unit of measure in pixels or percent for the Columns setting. The default value is "Percent". To change the value to "Pixels", select the Pixels icon.
Span Columns	In Detail Views and Activity Views , fields are typically displayed on the page in rows within a two-column table format. You can make a row containing a field span table columns by configuring the Span Columns setting. The default is true. When true, the row containing the field will span the columns of the table. When false, the row containing the field will be displayed within a table column and not span the columns of the table.

For instructions on how to configure a display type for a long string data type object field, see [“Configuring display types for long string fields \(Standard UI\)”](#) on page 358.

Configuring a display type for enumerated strings (Standard UI)

This is the procedure to configure a display type for object fields that have an Enumerated String data type. Enumerated strings can be displayed as lists, radio buttons, or check boxes.

For object fields that have an enumerated string data type, you can configure how enumerated string data displays to users on an object's details page. The display types for enumerated string data include lists, radio buttons, and check boxes.

Note: Changing the display type setting will affect the display of this field in all profiles.

Procedure

1. Access the **Profiles** page (see [“Accessing profiles”](#) on page 298).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type containing the object field you want to modify (for example, SOXControl).
4. On the **Object Fields** table for the selected object type, click the name of the object field to open its detail page.
5. On the **Object Field Information** table, click **Edit**.
6. On the edit page:

- a) To make the field required, select the **Required** box.

If a field is not required, to provide the ability to enter an empty value in the field:

- For radio buttons, a **None** option is automatically added to the set of radio buttons.
- For check boxes, the user would clear all check boxes.
- For lists, an empty selection is added to the list of choices.

When **None** is selected in a set of radio buttons, all check boxes are cleared, or the empty option in a list is selected, the value for the enumerated field will be blank.

Note: Field dependencies may mean a field is required even if **Required** is not selected. For details on field dependencies, see [“Dependent field behavior”](#) on page 278.

The **None** label can be changed and localized in the **Application Text | Labels | com.label.enum.selection.none** setting. For details on changing application text, see [“Localizing application text”](#) on page 564.

- b) To select a different display type, click the **Display Type** arrow and select a value from the list.

Select **List** to set the display as a list. Lists can be single selection or multiple value selection, depending on the **multi-value** setting for the field.

Select **Radio Button/Checkbox** to set the display type as radio buttons or check boxes. If the field is defined as **multi-value**, the display will use check boxes. If **multi-value** is not selected for the field, the display will use radio buttons.

For details on enumerated string data types, see [“Data types”](#) on page 203.

Chapter 13. Configuring the Task Focused UI

The Task Focused UI is a simplified user interface that is used by users and risk managers who need to complete tasks that are assigned to them and find information in OpenPages. The Task Focused UI is optimized for infrequent users who have access to targeted functionality in OpenPages.

Setting up the Task Focused UI

Before users can access the Task Focused UI, you must configure who can access it and define the views that are available.

Before you begin

Complete the following prerequisites:

- Learn about how users can interact with the Task Focused UI. For information, see *Getting started with the Task Focused UI* in the *IBM OpenPages with Watson User Guide*.
- Learn about the differences between the Task Focused UI and the Standard UI. For information, see [“Comparing the Standard UI and the Task Focused UI”](#) on page 365.
- Learn about views and how they are defined in the View Designer. For information, see [“Views in the Task Focused UI”](#) on page 370 and [“Using the View Designer”](#) on page 385.
- Learn about the GRC Workflow feature and plan how you will use it. Configure it after you configure the Task Focused UI with the exception of Task Views, which can be designed concurrently. For information, see [“Setting up GRC Workflow”](#) on page 495.

About this task

During the configuration process, plan and design what you want users to accomplish in the Task Focused UI. Then, define views that allow users to interact with OpenPages in a way that is tailored to your requirements.

Procedure

1. Update the permissions for role templates for administrators who are configuring the Task Focused UI.

- a) Click **Administration > Role Templates > <role template> > Role Permissions**.

- b) Select the **SOX > Administration > Task Focused UI** permission.

Administrators with this permission can define views with the  > **Solution Configuration > Views** task in the Task Focused UI.

In addition to **Views**, this permission also controls whether the  > **Other > Display debug info** task is displayed.

- c) Select the **SOX > Administration > Dashboards** permission.

Administrators with this permission can define dashboards with the  > **Solution Configuration > Dashboards** task in the Task Focused UI.

2. Update the permissions for role templates for users who access the Task Focused UI.

- a) Click **Administration > Role Templates > <role template> > Role Permissions**.

- b) Select the **SOX > Administration > User Interfaces > Login to Task Focused UI** permission.

All users have access to the Task Focused UI regardless of whether this permission is enabled. You must set the **Login to Task Focused UI** permission to enabled only for users who also access the Standard UI. This ensures that the URL launches the Task Focused UI.

3. Update the permissions for role templates for users who access the Standard UI.

a) Click **Administration > Role Templates > <role template> > Role Permissions**.

b) Select the **SOX > Administration > User Interfaces > Standard** permission.

- Users with the **Standard** permission can access the Standard UI in addition to the Task Focused UI.
- Users who do not have the **Standard** permission cannot access the Standard UI. When they use the Task Focused UI, the **Switch to Standard UI** menu item on the User menu in the Task Focused UI is hidden.
- By default, the **Standard** permission is set to enabled on all role templates and top level user-groups, for example, **Workflow, Reporting and Others**. To remove the **Standard** permission from users, verify the application permission on role templates and also on the user-groups that the user is a member of.

This video demonstrates how you configure role templates to control which user interface is initially displayed to users. It shows how to modify role templates in the Standard UI. However, role templates can also be modified in the Task Focused UI. For more information, see [“Modifying a role template” on page 115](#).

<https://youtu.be/XZ1XnL7MFqQ>

4. Verify permissions for role templates for users who access IBM Cognos Analytics from the Task Focused UI.

a) Click **Administration > Role Templates > <role template> > Role Permissions**.

b) Select the **SOX > Administration > CommandCenter Studios > Cognos Analytics** permission.

Users with this permission can access the IBM Cognos Analytics through the **Analytics** link in the banner. The link is hidden for users who do not have this permission.

5. Review the URLs that launch OpenPages.

- For a URL in the format `https://<server>:<port>/openpages/app/jspview/react/grc`
 - All users are directed to the Task Focused UI.
- For a URL in the format `https://<server>:<port>/openpages`
 - Users with only the **Standard** permission are directed to the Standard UI.
 - Users with both the **Login to Task Focused UI** permission and the **Standard** permission are directed to the Task Focused UI.
 - All other users are directed to the Task Focused UI.
- For a URL in the format `https://<server>:<port>/openpages/home.do`
 - Users with the **Standard** permission are directed to the Standard UI.
 - Users without the **Standard** permission are directed to the Task Focused UI.

Users who can access both interfaces might want to bookmark a URL in this format because a URL in the `https://<server>:<port>/openpages` format directs them to the Task Focused UI.

The URL redirects are applied in the same way in an environment where single sign-on (SSO) is enabled. No additional configuration is required for SSO.

6. Review profiles for users who will use the Task Focused UI. A user's profile in the Standard UI is also used in the Task Focused UI.

7. Review views in the Standard UI. Some aspects of views that are defined in the Standard UI are also used in Task Focused UI. For example, the **Filter on all fields in profile** setting controls fields that are available to users when they define private filters in Grid Views. For more information, see [“Advanced filters field configuration for Filtered List View” on page 629](#).

8. Define default dashboards for profiles. For more information, see [“Home page, dashboard, and tabs in the Task Focused UI” on page 367](#) and [“Defining a dashboard for a profile” on page 368](#).
9. Plan the views that are used in the Task Focused UI. For information, see:
 - [“Planning the Grid Views” on page 373](#)
 - [“Planning the Creation Views” on page 376](#)
 - [“Planning the Task Views” on page 380](#)
10. Define the views that are used in the Task Focused UI. For information, see:
 - [“Defining a Grid View” on page 389](#)
 - [“Defining a Creation View” on page 391](#)
 - [“Defining a Task View” on page 394](#)
11. Optional: Customize the Primary menu.
For more information, see [“Customizing the Primary menu” on page 446](#).
12. Optional: Configure IBM Watson Assistant . For more information, see [“IBM Watson Assistant ” on page 1013](#).
13. Optional: Configure a Net Promoter Score survey. For more information, see [“Configuring a Net Promoter Score \(NPS\) survey” on page 450](#).

Comparing the Standard UI and the Task Focused UI

The two user interfaces in OpenPages are intended for different purposes and audiences. Use the appropriate one for the work you need to accomplish.

The Standard UI is the user interface that has been part of OpenPages for numerous releases. Users and administrators use it to have full access to all the functionality and administration tasks in OpenPages.

The Task Focused UI is an optional secondary and highly simplified user interface that users access to complete their daily tasks. It is designed for the first line of defense and for users who are not familiar with OpenPages and do not require training. The Task Focused UI is easy to use and hides much of the functionality of OpenPages from the user.

In a typical OpenPages implementation, some users can access only the Task Focused UI, some users and administrators can access only the Standard UI, and some users and administrators can access both.

The information in this guide applies to the Standard UI unless otherwise noted.

The following table describes the differences between the Task Focused UI and the Standard UI.

<i>Table 143. Differences between the OpenPages user interfaces</i>		
Feature	Standard UI	Task Focused UI
Home page	Yes	Yes
Personalized dashboard	Yes	Yes but enhanced
My Work tab	Yes	No
My Tasks tab	No	Yes
Subscription Tasks tab	No	Yes
Oversight Tasks tab	No	Yes
My OpenPages menu	Yes	No
Process Portal	Yes	No
Reports	Yes	Yes
Changing reporting periods	Yes	Yes

Table 143. Differences between the OpenPages user interfaces (continued)

Feature	Standard UI	Task Focused UI
Defining reporting periods	Yes	Yes
Filters	Yes	Yes
% (percent symbol) (wildcard in search boxes)	Yes	No
Adding objects	Yes	Yes but simplified
Deleting objects	Yes	Yes
Locking and unlocking objects	Yes	Yes
Associating objects	Yes	Yes but simplified
Editing information	Yes	Yes but simplified
Adding files (attachments)	Yes	Yes but simplified
Supporting multiple versions of the same file (attachment)	Yes	Yes
Global search	Yes	Yes (as a dashboard panel)
Watson Discovery Analyze API	No	Yes
Watson Natural Language Classifier	Yes	Yes
Dependent fields	Yes	Yes
Dependent picklists	Yes	Yes
Rules-based dependent fields	No	Yes
Changing the value in a picklist controller field (in a dependent picklist)	Inconsistent values in dependent fields are automatically cleared	Inconsistent values in dependent fields are flagged as invalid
Computed fields	Yes	View only
Card layouts, chart diagrams, counts, grid layouts, and tree diagrams (by using relationship fields)	No	Yes
Inline guidance	No	Yes
User guidance	No	Yes
Field guidance	Yes	Yes
Colors for enumerated values	No	Yes

Table 143. Differences between the OpenPages user interfaces (continued)

Feature	Standard UI	Task Focused UI
Colors for number ranges	No	Yes
Business entity selector fields	Yes	Yes
Recently Used tab	Yes	No
Change history/audit log	Yes	Yes (the Activity tab on Task Views)
IBM Watson Assistant	No	Yes
Net Promoter Score (NPS) survey	No	Yes
IBM Watson Language Translator	No	Yes

Home page, dashboard, and tabs in the Task Focused UI

The Home page is the initial page that users see when they log in to OpenPages.

The Home page organizes information and tasks. It contains three parts:

- A dashboard
- Task tabs
- Tabs for reports

Dashboard on the Home page

The dashboard displays panels with content that is personalized for each user.

Dashboard panels in the Task Focused UI can come from the following sources:

- Users can define their own dashboard panels in the Task Focused UI. On the Home page, a user clicks



to open the Dashboard configuration menu.

For more information about how users add panels to the dashboard in the Task Focused UI, see the *IBM OpenPages with Watson User Guide*.

- Administrators can define dashboards in the Task Focused UI that apply to specific profiles. In this way, users have a default dashboard based on the profile that they belong to. The dashboards are consistent and standardized across a group of users. Users can still customize their dashboard by adding their own dashboard panels or hiding dashboard panels that are defined on the default dashboard.

For more information, see [“Defining a dashboard for a profile” on page 368](#).

- Users can define their own dashboard panels in the Standard UI. Dashboard panels that a user has defined in the Standard UI are brought over to the dashboard in the Task Focused UI with the exception of panels for global search.

Dashboard panels that are defined in the Standard UI are displayed in the Task Focused UI the first time a user signs on to the Task Focused UI. Subsequent changes to dashboard panels that are defined in the Standard UI are not brought over to the dashboard in the Task Focused UI.

For more information about how users add panels to the Dashboard tab in the Standard UI, see the *IBM OpenPages with Watson User Guide*.

Dashboard panels that are defined by profile in the Standard UI do not display on dashboards in the Task Focused UI.

Task tabs on the Home page

The following task tabs display on the Home page:

- My Tasks tab

The My Tasks tab summarizes the tasks that belong to a user.

- Subscription Tasks tab

The Subscription Tasks tab summarizes the tasks that a user is subscribed to.

- Oversight Tasks tab

The Oversight Tasks tab summarizes the tasks for which a user has oversight responsibility.

The content and layout of each tab is fixed and cannot be changed. For more information about the task tabs, see the *IBM OpenPages with Watson User Guide*.

Tabs on the Home page for reports

A dashboard can contain up to three tabs for Cognos and OpenPages reports.

The reports must already exist and must be added to the profile. Two methods can be used to create tabs for reports: users can define report tabs on their dashboard and administrators can use the **Manage Dashboards** task in the Task Focused UI.

For more information, see the *IBM OpenPages with Watson User Guide* and [“Defining a dashboard for a profile” on page 368](#).

Defining a dashboard for a profile

A dashboard can contain multiple panels and up to three tabs for Cognos and OpenPages reports. A dashboard that is defined for a profile provides a default dashboard for all users that belong to that profile.

Before you begin

See the *IBM OpenPages with Watson User Guide* for information about to configure dashboard panels, including charts, filter counts, and other widgets, in the Task Focused UI.

Review filters for object types that are used in dashboard panels. For a filter to be available in a dashboard panel, it must meet both of the following criterion:

- The filter must be associated to the object type.

For more information, see [“Tasks to define filters for an object type” on page 267](#).

- The filter must be associated to a filtered list view on the object type on your profile.

For more information, see [“Associating filters to Filtered List view and Grid view pages” on page 334](#).

Keep the number of panels on the dashboard reasonable. A dashboard with many panels can potentially take longer to load.

If they exist, review the dashboard panels that are defined by profile for the Standard UI. These dashboard panels are not brought over to the Task Focused UI. But you can use them as a conceptual starting point for defining dashboards by profile for the Task Focused UI. For more information, see [“Configuring users' Dashboard tabs” on page 319](#).

To add tabs for reports, two conditions must be met:

- The reports must already exist. For more information about creating reports, see [“OpenPages with Watson V6 folder reports” on page 167](#)

- The reports must be added to the profile. For more information, see [“Adding reports to a profile” on page 305](#). In the Standard UI, open the profile and verify that the reports are listed on the Home Page Tab Configuration tab.

About this task

A dashboard must be marked as active for the panels to appear on users' dashboards.

Multiple dashboards can exist for that same profile. If more than one dashboard is marked as active, the last published dashboard is the one that is displayed on users' dashboards.

Click  to access a search filter. You can search by the active setting and profile. You can also click in the search box and enter free text. The search box is based on dashboard name, profile, and description.

Dashboards can be migrated from one environment to another environment using Export Configuration and Import Configuration or the ObjectManager tool. For more information, see [“Exporting and importing dashboards” on page 452](#).

Procedure

1. Click  > **Solution Configuration** > **Dashboards**.
2. Click **Add New**.
3. Enter a **Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
4. Set **Active** to true or false.
5. Select a **Profile** that the dashboard applies to.
6. Optional: Enter a **Description**.
7. Click **Add**.
The dashboard is added to the list of dashboards.
8. Click the dashboard name.
9. Click  to open the Dashboard configuration menu.
10. Click **Add Panel** and begin defining the panels for the dashboard. See the *IBM OpenPages with Watson User Guide* for more information.
11. Click **Add Tab** to add tabs for reports.
 - a) Enter a **Name**.
 - b) Enter a **Label**. Keep it short. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

- c) Select a **Report Type**.
 - d) Click **Done**.
The report tab is added. A dashboard can have up to three report tabs. Click a tab and move it to where you want it to display. Tabs can be removed, if needed.
12. Click **Done**.
 13. Click **Publish**.
 14. Test the dashboard. Each time you change the dashboard, you need to publish it and retest it.

Changes to profiles can affect dashboards. If an object type, filter, or chart field is removed from a profile, the dashboard panels and content will change. If the profile change affects a panel as a whole, for example, an object type is removed from a profile, then the panel is removed. If the profile change affects only a single widget in a custom panel, then the widget is removed. This can cause an empty panel to display on a dashboard. You can either repopulate the custom panel with other widgets or delete it.

If the Dashboard encounters a problem and cannot render, you can apply safe mode by adding ?safeMode=1 to the end of the URL. The rendering process stops and you can access the dashboard configuration to debug the problem. Remove ?safeMode=1 from the URL to exit safe mode.

Adding a Search panel

A Search panel on a dashboard provides a means to use global search in the Task Focused UI.

Before you begin

Global search is a powerful feature for finding information. To learn more about it, see the *IBM OpenPages with Watson User Guide*.

Global search must already be configured. For more information, see [Chapter 20, “Configuring the global search feature,”](#) on page 649.

About this task

When a user enters text in a Search panel, global search analyzes the input and displays matching results. Up to 25 objects can be returned in a Search panel. If a user clicks an object in the Search panel result list, the object opens in a new tab. The user can also mark an object as a favorite.

Consider your usability and performance when you design the Search panels. A Dashboard may need to contain one Search panel that can search across all objects. It may also need one or more Search panels that are targeted to specific objects types that users access most frequently. For these Search panels, set values in **Object Type** and Folder Picker so that the search is restricted to a smaller set of objects.

Procedure

1. Create a dashboard panel and complete the steps up to adding a panel. For more information, see [“Defining a dashboard for a profile”](#) on page 368.
2. Click **Add Panel**.
3. Select **Search** in **Panel Type**.
4. Enter a **Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
5. Enter a **Label**. The label displays as a title for the panel.
6. Set **Object Type** to *All object types* or select one or more object types to restrict the search to specific object types. Be sure to select File in **Object Type** if you want to include file attachments descriptions and content in the search.
7. Optional: Click **Choose** and select one or more folders in Folder Picker.
8. Click **Done**.
9. Click **Done**.
10. Click **Publish**.
11. Test the search panel. Each time you change the dashboard, you need to publish it and retest it.

What to do next

If it does not already exist, add a favorites panel to the dashboard so that users can access the objects they mark as favorites.

Views in the Task Focused UI

Views in the Task Focused UI control what information is displayed to users and how they interact with OpenPages.

When you configure the Task Focused UI, you configure views that users access. You design the content and layout of a view by using the View Designer in the Task Focused UI.

Prerequisite

Before you plan and design the views, learn about the UI components in the Task Focused UI. For information, see *Navigating the Task Focused UI* in the *IBM OpenPages with Watson User Guide*.

Show me how

This video provides an overview of views and the View Designer.

<https://youtu.be/R7ytoazgwg4>

Grid Views, Creation Views, and Task Views

The Task Focused UI uses three types of views:

- Grid Views

For more information, see [“Planning the Grid Views” on page 373](#).

- Creation Views

For more information, see [“Planning the Creation Views” on page 376](#).

- Task Views

For more information, see [“Planning the Task Views” on page 380](#).

For each type of view, there can be:

- system views
- custom views

System views

System views are read-only views that are provided with OpenPages to get you started. You can use them as they are and as templates and learning tools for custom views that you create on your own.

For each object type, OpenPages provides at least one system Grid View, one system Creation View, and one or more system Task Views.

For a system view, you can:

- set the **View Priority**
- make it enabled
- make it disabled if you no longer use the view
- make it a default view

You cannot modify or delete a system view. However, you can create a custom view that is a copy of a system view. For more information, see [“Creating a custom view from a system view” on page 398](#).

For system views, in the View Designer you can view the **JSON** tab but the **Design** tab is hidden. To view a system view in the **Design** tab, copy it to a custom view and open the **Design** tab in the custom view.

Custom views

Custom views are views that you create on your own. You can create them for all object types and all view types.

For a custom view, you can:

- Customize the content of the view to your specific requirements
- Set the **View Priority**
- Make it enabled
- Make it disabled if you no longer use the view

- Make it a default view

For custom views, in the View Designer you can design the view on the **Design** tab. There is no need to use the **JSON** tab except to copy views.

Controlling what views are displayed to users

You use rules on Grid Views, Creation Views, and Task Views to control what views are displayed to users. You can define one or multiple Grid Views, Creation Views, and Task Views for an object type.

For simplicity, the explanation below describes how to control what Creation Views are displayed to users. The same logic applies to Grid Views and Task Views.

If you define one Creation View for an object type, you select **Use as default view for this object type for all profiles** on the view.

If you define multiple Creation Views for an object type, you define Creation Views where **Use as default view for this object type for all profiles** is cleared and rules determine what view is displayed to a user. You must still define one Creation View that is the default. For this view, you select **Use as default view for this object type for all profiles**.

Creation Views with rules take precedence over the default Creation View. The default Creation View is displayed if none of the Creation Views with rules match for a user after the rules have been checked.

View Priority on default views is always set to 1 and cannot be changed. **View Priority** on default views is disregarded during this selection.

Combining field types from the Standard UI and the Task Focused UI

Views in the Task Focused UI are built by combining field types that are defined in the Standard UI and field types that are defined only in the Task Focused UI.

Field types in the Standard UI

Field types that are defined in the Standard UI can be added to views in the Task Focused UI.

You can, in some cases, add functionality. For example, a number field that is defined in the Standard UI can be displayed in the Task Focused UI as a progress bar. The field must be defined in the Standard UI with a minimum and maximum, for example, 0-100, 0-10, 0-1. You add the field to a view in the Task Focused UI and set **Display Type** to Progress. You can optionally add color ranges.

You can also override functionality. For example, you can define a field as required in a view in the Task Focused UI even if it is defined in the field definition or profile in the Standard UI as not required. To make a field required in a view, you set **Required** for the field to `true`. If the field is in multiple views, you can set **Required** differently in each view. The only limitation is that you cannot set **Required** to be less restrictive than how it is defined in the Standard UI. You can use the **Read Only** in the same way with the same limitation.

Similarly, field dependencies that are defined for a field in the Standard UI are also used in views in the Task Focused UI. You do not have to include a dependency's controlling fields in a view for it to work. You cannot override or remove dependencies in the Task Focused UI, but you can add new ones by using rules. For more information, see [“Configuring rules” on page 439](#).

Field types in the Task Focused UI

Three field types are unique to views in the Task Focused UI: relationship, group, and help fields. These field types do not exist in the Standard UI.

For information about relationship type fields, see [“Adding and configuring relationship fields on views” on page 413](#).

For information about group type fields, see [“Arranging fields in columns”](#) on page 400.

For information about help type fields, see [“Adding inline guidance”](#) on page 400.

Planning the Grid Views

Determine what Grid Views you want to use for each object type.

Define the Grid Views by using the following methods:

- Use a system Grid View as is.
- Make a copy of a system Grid View and modify the copy to meet your requirements.
- Make a copy of a published custom Grid View and modify the copy to meet your requirements.
- Make a copy of a Filtered List View from the Standard UI and modify the copy to meet your requirements in the Task Focused UI.
- Define a Grid View from scratch.

For information, see [“Defining a Grid View”](#) on page 389.

Using a Grid View

A Grid View shows a list of objects for a selected object type and allows you to filter, search, and select a specific object.

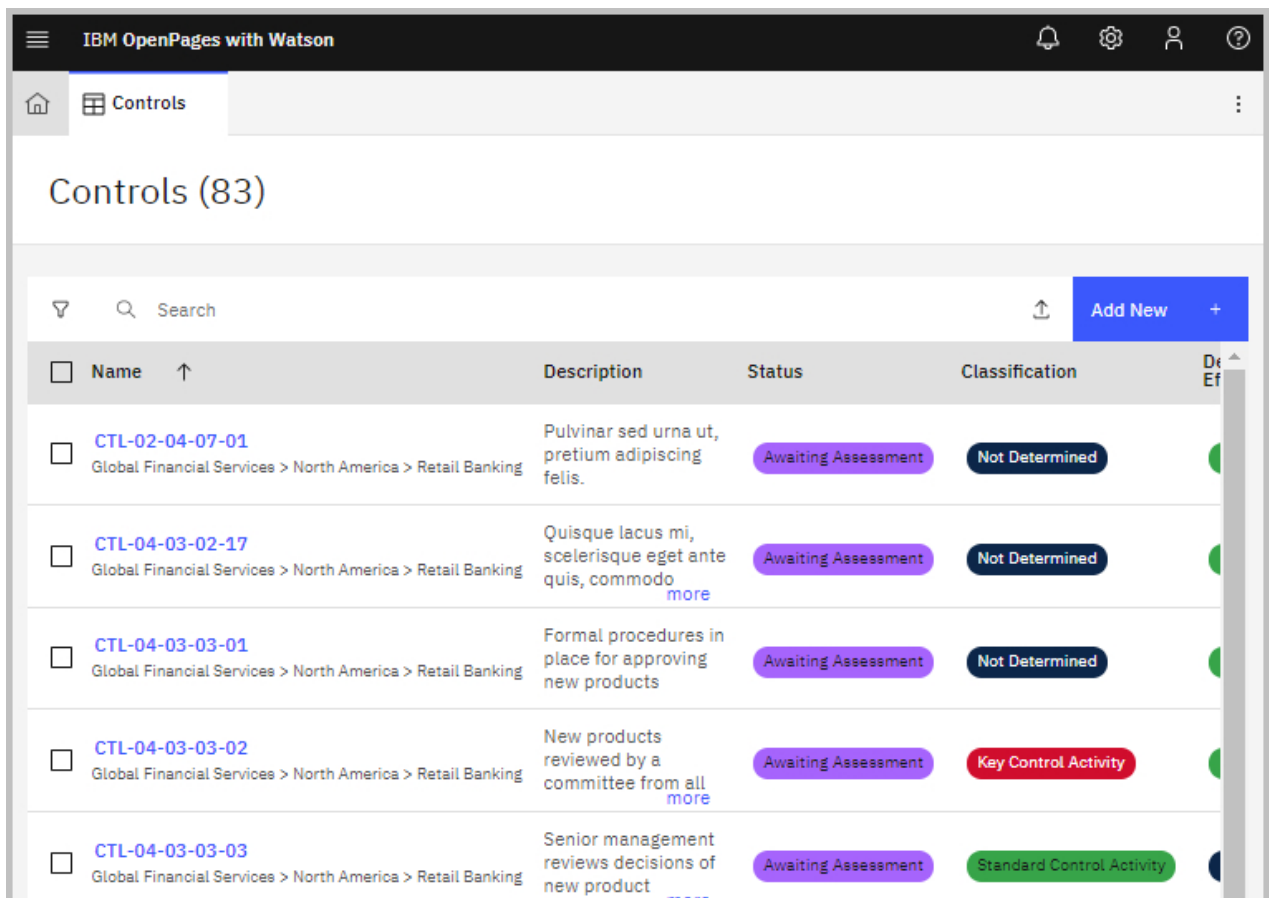
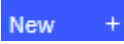


Figure 20. Example of a Grid View

When you select an object type from the Primary menu, the dashboard, or a Task View, a Grid View is displayed.

In a Grid View, you can take the following actions:

- Select an object that you want to work with and open it.
- Click in the search box, enter free text. and press Enter. All objects that contain the text are returned.
- Click in the search box, enter specific values for enumerated fields, and press Enter. You can also build a list of selection criteria for multiple values and multiple fields.
- Click  to access public and private filters.
- Clear the **Active Only** check box, if it is displayed, to show objects that have completed a workflow. You can overwrite the **Active Only** filter or create your own default filters for object types that do not use workflows.
- Select one or more objects with the check mark and then you can delete, lock, unlock, move, and export them (depending on the object type and permissions).
- Select one or more objects with the check mark and then you can update field values by clicking  (bulk update). The fields that allowed to be updated are configured in the view.
- Click a field name in the header row to sort the list by that field in ascending order. Click the field name again to choose descending order.
- Click  to create a new object. Whether the icon is displayed depends on how your system is configured.
- Choose a value in **Items per page** to control how many objects are listed on a single page.

A Grid View lists objects for a single object type. Unlike grid views in the Standard UI, users cannot edit a Grid View in the Task Focused UI.

Grid Views for bulk workflow actions are Grid Views but with some differences in functionality due to their access point. For more information, see [“Defining Grid Views for bulk workflow actions” on page 390](#).

Designing a Grid View

A Grid View contains fixed and configurable UI components.

Controlling what Grid View is displayed to a user

An object type can have multiple Grid Views that are enabled. You define rules that determine what Grid View is displayed to a user. A Grid View can be displayed:

- For all or specific profiles.

For more information, see [“Controlling what views are displayed to users” on page 372](#) and [“Defining a Grid View” on page 389](#).

When users access an object type that does not have an enabled, valid Grid View, an error is displayed.

Designing a Grid View for scalability and performance

Consider scalability and performance when you design Grid Views. For example, if there are 500,000 Control objects in a library, a Grid View for Controls can be slow to display if no filters are applied.

For quicker system performance, apply a default filter to Grid Views that are defined for object types that potentially display a large number of objects.

For more information, see [“Defining default filters on Grid Views” on page 406](#).

Fixed UI components in a Grid View

Table 144. Fixed UI components in a Grid View	
UI component	Description
Work area	The work area (the grid) is always displayed.

Table 144. Fixed UI components in a Grid View (continued)

UI component	Description
Filter icon ()	Is always displayed and cannot be hidden.
The name of the object type	Is always displayed and cannot be hidden.
The number of objects returned	Is always displayed and cannot be hidden.
The Search box	Is always displayed and cannot be hidden.
Add New icon	Is displayed if creation is allowed at the object level and per the user's access permissions.
Checkboxes next to objects	Are always displayed and cannot be hidden.
The word <i>more</i>	Is always displayed when text is longer than can be shown. It cannot be hidden.
Items per page	Is always displayed and cannot be hidden.

Configurable UI components in a Grid View

Table 145. Configurable UI components in a Grid View

UI component	Description
Work area	The work area (the grid) consists of columns and rows. You can configure how many columns are displayed and what fields display in each column. The header row in the grid is always displayed. The content of the rows is determined by the data that the user filters.
Display alternate field labels	You can change the locale to display alternate field labels. For information, see “Applying alternate field labels” on page 405.
Default filter	If the object type has workflows, the Active Only check box displays. You can optionally overwrite the Active Only filter. If the object type does not have workflows, you can create your own default filter. For information, see “Defining default filters on Grid Views” on page 406.
Add New icon	Is displayed if creation is allowed for the object type and the user has access permissions for the object type.

Table 145. Configurable UI components in a Grid View (continued)

UI component	Description
The  (Bulk Update) icon	Is displayed if registry settings that control bulk update functionality are configured for the user and object type. For more information, see: • “Disable Bulk Update link in the Task Focused UI” on page 630 • “Exclude object types in Filtered List Views from bulk updates” on page 631 • “Hide the Bulk Update feature in filtered list views for user profiles” on page 631 The fields that are allowed to be updated are configured by the Bulk update setting in the view definition. Fields that are not displayed in the Grid View can also be updated, if configured. Bulk update is not available for read only fields, for example, computed fields, workflow fields, and system fields that are read only. Administrators with the Bulk Update All Fields application permission can bypass the restrictions on fields that can be updated. For more information, see “Types of application permissions” on page 91.
Defining colors for enumerated field values	You can add colors to values in enumerated field values. For information, see “Apply colors to enumerated field values” on page 407.
Applying color ranges	You can apply colors to value ranges for numbers, currencies, and counts on relationship fields. For information, see “Apply colors to value ranges” on page 408.

Planning the Creation Views

Determine what Creation Views you want to use for each object type.

Define the Creation Views by using the following methods:

- Use a system Creation View as is.
- Make a copy of a system Creation View and modify the copy to meet your requirements.
- Make a copy of a published custom Creation View and modify the copy to meet your requirements.
- Make a copy of a Detail View from the Standard UI and modify the copy to meet your requirements.
- Define a Creation View from scratch.

For information, see [“Defining a Creation View” on page 391](#).

Using a Creation View

A Creation View is used to define new objects.

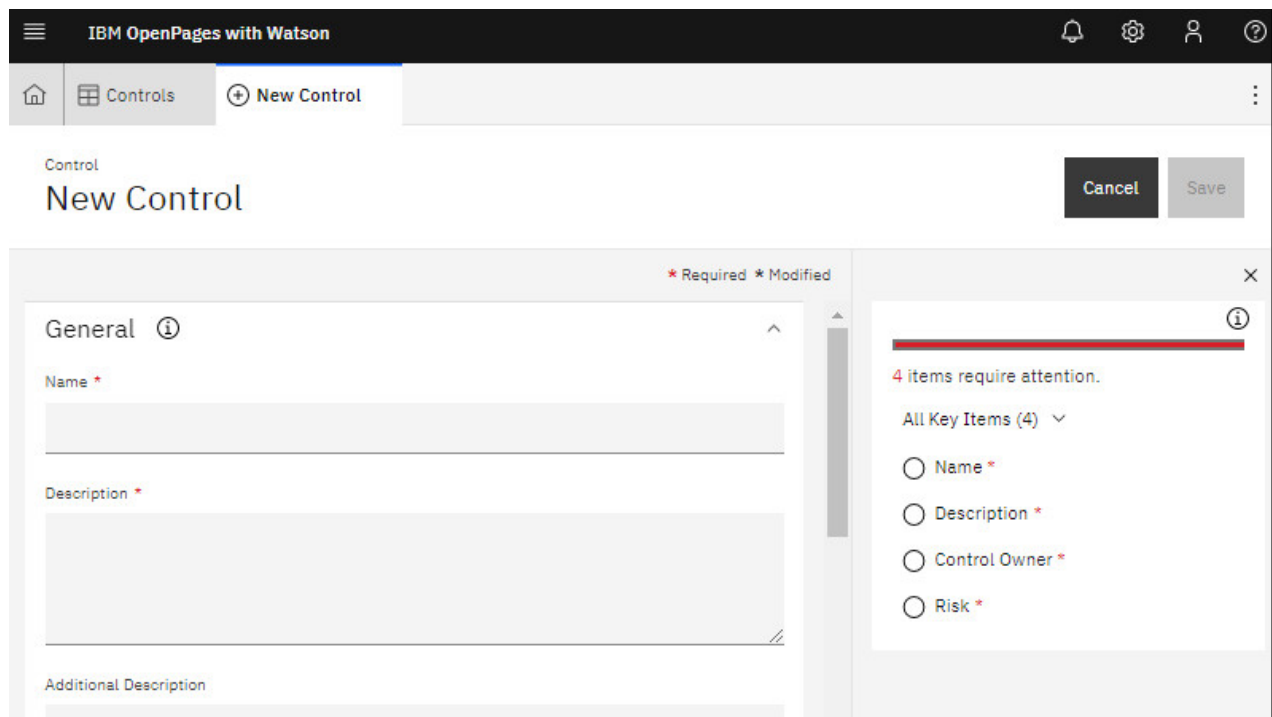


Figure 21. Example of a Creation View

A Creation View is displayed when you click **New** + from the dashboard, a Grid View, or a Task View. The icon might be named differently, depending on your configuration.

To use a Creation View, you complete the fields in the view and save the object. At a minimum, you must provide values in required fields.

A primary parent object is required for most object types. Depending on the access point and how the views are defined, the parent object can be defaulted or you might be required to provide one. For example, when you click **Add New** from a Grid View for Issues, you are required to provide a parent object such as a Control. From this access point the parent object is not known and you must provide it. However, if you are on a Task View for a Control and create a child Issue object, the parent object can be defaulted from the Task View and you must not select it.

Most Creation Views must provide a means for the selection of a primary parent since a parent object is required for most object types.

Creation Views for adding files (system and non-system) must provide a means to upload a file. For more information, see [“Defining Creation Views for file object types”](#) on page 393.

Designing a Creation View

A Creation View contains fixed and configurable UI components.

Controlling what Creation View is displayed to a user

An object type can have multiple Creation Views that are enabled. You define rules that determine what Creation View is displayed to a user. A Creation View can be displayed:

- For all or specific profiles.
- For one or more parent object types if the parent object is known.
- For any parent object types if the parent object is known.

Most Creation Views must provide a means for the creation of a primary parent since a parent object is required for most object types. The access point determines how the parent object can be provided:

- For Creation Views that are accessed by clicking **Add New** from a Grid View, the parent object is not known and the view must contain a relationship field that allows a user to select a parent object.
- For Creation Views that are accessed from a relationship field in a Task View, the parent object is known since the object is open. The view need not contain a relationship field that allows a user to select a parent object. For these Creation views, you can define a rule in **Parent Types (if not specified, view is valid for all parent types)**. The rule can be defined for one or more specific parent object types, or any parent object types.

Utilize this feature in Creation Views for two reasons:

- So that users need not select a parent object. This makes the view easier to use because selecting objects is time consuming and unnecessary because the parent object is known.
- So that different Creation Views can be displayed based on the parent object type. For example, a Creation View for an Issue can be different depending on whether it is accessed from a parent object that is a Control versus a Resource.

For more information, see [“Controlling what views are displayed to users” on page 372](#) and [“Defining a Creation View” on page 391](#).

When users access an object type that does not have an enabled, valid Creation View, no view is displayed. Users can close the page or switch to the Add New wizard in the Standard UI.

Associating a primary parent object and parent/child objects

For most object types, a Creation View must provide the ability to associate a primary parent object. This can happen in two ways:

- A Creation View can require the user to manually select a parent object.

To do this, you add a card or grid relationship field with an **Associate Primary Parent** action to a Creation View. Set the **Required** property on the relationship field to `true` to make the field mandatory.

- A Creation View can take over the parent object from the access point where the user starts.

To do this, you define a rule for the Creation View in **Parent Types (if not specified, view is valid for all parent types)**. The rule can be defined for one or more specific parent object types, or any parent object types. The Creation View need not contain a relationship field that adds a parent object.

Creation Views might also provide the ability to associate one or more parent or child objects. To do this, add a card or grid relationship field with an **Associate** action to a Creation View

If a Creation View allows users to associate both a primary parent object and parent objects, you can either define two relationship fields, one with the **Associate Primary Parent** action and one with the **Associate** action for parents, or you can define one relationship field with two actions, **Associate Primary Parent** and **Associate**.

In the former case, two relationship fields, you can make the relationship field with the **Associate Primary Parent** action required to ensure that users provide a primary parent.

In the latter case, one relationship field with two actions, you can make the relationship field required but you cannot ensure that a user provides a primary parent object. Therefore, the first object that is listed in the Grid View becomes the primary parent when the object is saved. This is true even if the user did not specifically choose a primary parent using **Associate Primary Parent**.

You can use rules on relationship fields to help a user select the correct associations. You can use the visible and hidden rules on a relationship field to show or hide a relationship field based on the value of another field in the view. For example, if you create an Issue, the issue type that the user chooses can determine the parent object type that is displayed.

For more information about relationship fields, see [“Adding and configuring relationship fields on views” on page 413](#).

Creation Views for adding files

Creation Views for adding files (system and non-system) must provide a means to upload a file. For more information, see [“Defining Creation Views for file object types”](#) on page 393.

Fixed UI components in a Creation View

Table 146. Fixed UI components in a Creation View	
UI component	Description
Work area	The work area is always displayed.
	The Save icon is always displayed and cannot be hidden. It is clickable after all required information for an object has been entered.
	The Cancel icon is always displayed and cannot be hidden.
Object type and New [object type]	The name of the object type is always displayed in the header.
	Field guidance for each section is displayed if at least one field in the section is defined with a field description.
	The search icon is always displayed. Use it to search for fields in the view.

Configurable UI components of a Creation View

Table 147. Configurable UI components in a Creation View	
UI component	Description
Work area	You configure the content of the work area by defining sections and adding fields to each section.
Inline guidance	You can add inline guidance. For information, see “Adding inline guidance” on page 400.
User guidance	You can add user guidance that includes information text and a list of key fields. For information, see “Adding user guidance” on page 402.
Adding fields to sections	Fields are organized in sections. For information, see “Adding a section” on page 399.
Organizing fields into columns	You can organize fields in columns. For information, see “Arranging fields in columns” on page 400.
Defining colors for enumerated field values	You can add colors to values in enumerated field values. For information, see “Apply colors to enumerated field values” on page 407.
Applying color ranges	You can apply colors to value ranges for numbers, currencies, and counts on relationship fields. For information, see “Apply colors to value ranges” on page 408.

Table 147. Configurable UI components in a Creation View (continued)

UI component	Description
Displaying alternate field labels	You can change the locale to display alternate field labels. For information, see “Applying alternate field labels” on page 405 .
Associating objects	You can add the ability to associate objects, for example, associate a primary parent to a new object. For information, see “Adding a card layout” on page 414 and “Adding a grid layout” on page 425 .
Organizing relationship fields in tab groups.	“Organizing relationship fields in tab groups” on page 433
Accessing a natural language processing service	You can provide the ability to make suggestions by using a natural language processing service. For information, see “Adding a classifier field that makes taxonomy suggestions” on page 410 . For information, see “Adding a classifier field that makes object association suggestions” on page 430
Adding URL links	You can add URL fields that display as buttons or links. For information, see “Displaying a URL launcher field as a button or link” on page 410 .
Uploading files	You can add the ability to upload files to Creation Views for file object types. For information, see “Defining Creation Views for file object types” on page 393 .

Planning the Task Views

Determine what Task Views you want to use for each object type.

Define the Task Views by using the following methods:

- Use a system Task View as is.
- Make a copy of a system Task View and modify the copy to meet your requirements.
- Make a copy of a published custom Task View and modify the copy to meet your requirements.
- Make a copy of a Detail view from the Standard UI and modify the copy to meet your requirements in the Task Focused UI.
- Define a Task View from scratch.

For information, see [“Defining a Task View” on page 394](#).

Using a Task View

A Task View is used to complete work that has been assigned to you.

IBM OpenPages with Watson

Issue: Policy needs update

Issue Status: Issue Status

Priority: Low

Action Items: 0

Cancel Save

Task Activity

Reveal editable fields: Off

* Required * Modified

General

Name: Policy needs update

Assignee:

Description: All Inventory policy documents need to be translated and uploaded into FCM for the locales to which they apply. Adding a detailed Description improves IBM Watson suggestions.

Controls

Select Primary Control Select Additional Controls ISO Control Suggestions (1)

There are no Controls

Priority: Low

Issue Status:

Issue Category:

Risk Domain:

Deficiency Details

Issue Owner: Search users (This value is required.)

Issue Approver:

Issue In Progress

Stage: In progress

Due Date: 9/14/2020

Select an action to validate

1 item requires attention.

All Key Items (7)

- Name
- Description
- Issue Category
- Issue Owner
- Issue Approver
- Priority
- Due Date

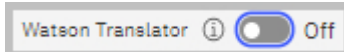
Figure 22. Example of a Task View

You open a Task View from the following access points:

- In a Grid View, you select an object and open it.
- In a report, you click an object and open it.
- In a Task View, you can open another Task View.

In a Task View, you can take the following actions:

- Review information about the object.
- Click  to view field guidance for fields in a section.
- Click the **Activity** tab to view change history.



- If it is displayed, click [Watson Translator](#) to translate values in text fields to the language associated to your locale. For more information, see [“IBM Watson Language Translator” on page 1018](#).

Depending on how the Task View is configured, you might also be able to take the following actions:

- Use the inline guidance and user guidance to help you understand what you need to do.
- Change information about the object.
- Associate the object to another object.
- Disassociate an object from another object.
- Create objects.
- Delete objects.
- If **Select an action to validate** is displayed in user guidance, you can check whether an action would pass validation before you complete the action.
- Choose an action, for example, Approve or Reject, to complete the task.
- Use Watson Moments to help you make object associations.
- Add a comment (reason) when you choose an action, if a comment window is displayed. The comment can be required or optional.
- View a tree structure that displays the object's relationship to other objects and navigate through the structure.
- View information about the object in a chart and navigate into the chart.
- View information about the object in a card or grid and navigate through to the objects in the card or grid.
- View cards, grids, charts, and trees that are organized in tab groups. For more information, see [“Organizing relationship fields in tab groups” on page 433](#).
- Add file attachments. For more information, see [“Defining Task Views for file object types” on page 395](#).
- Open and edit Microsoft Office files, if configured. For more information, see [“Defining Task Views for file object types” on page 395](#).

Designing a Task View

A Task View contains fixed and configurable UI components.

Controlling what Task View is displayed to a user

An object type can have multiple Task Views that are enabled. You define rules that determine what Task View is displayed to a user. A Task View can be displayed:

- For all or specific profiles.
- If the value of an enumeration field on an object is a specific value.
- If the signed on user matches the value of a user field, for example, is the owner or assignee.

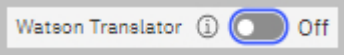
For more information, see [“Controlling what views are displayed to users” on page 372](#) and [“Defining a Task View” on page 394](#).

When users access an object type that does not have an enabled, valid Task View, no view is displayed. Users can close the page or switch to a Detail View or Activity View in the Standard UI.

Task Views for adding and managing files

Task Views are used to support adding and managing files. For more information, see [“Defining Task Views for file object types” on page 395](#).

Fixed UI components in a Task View

Table 148. Fixed UI components of a Task View	
UI component	Description
Task View header	A Task View header is always displayed. The object type and object name are always displayed in the Task View header and cannot be hidden.
Work area	The work area is always displayed.
Activity tab	The Activity tab is displayed if a user has the Audit Trail (Change History) application permission.
	Field guidance for each section is displayed if at least one field in the section is defined with a field description.
	The search icon is always displayed. Use it to search for fields in the view.
Icons for IBM Watson Language Translator	If IBM Watson Language Translator has been configured for the current object type and the signed on user has the Watson Language Translator UI permission, the  icon displays in Task Views. It displays regardless of whether there is text that can be translated. The icon requires no configuration in Task Views. For more information, see “IBM Watson Language Translator” on page 1018.

Configurable UI components in a Task View

Table 149. Configurable UI components of a task view	
UI component	Description
Task View header	You can configure fields and the Actions button in the Task View header. For information, see “Defining a Task View header” on page 404.
Work area	You configure the content of the work area by defining sections and adding fields to each section.
Inline guidance	You can add inline guidance. For information, see “Adding inline guidance” on page 400.
User guidance	You can add user guidance that includes information text, a list of key items, and the ability to validate actions. For information, see “Adding user guidance” on page 402.
Adding fields to sections	Fields are organized in sections. For information, see “Adding a section” on page 399.
Organizing fields into columns	You can organize fields in columns. For information, see “Arranging fields in columns” on page 400.

Table 149. Configurable UI components of a task view (continued)

UI component	Description
Defining colors for enumerated field values	You can add colors to values in enumerated field values. For information, see “Apply colors to enumerated field values” on page 407 .
Applying color ranges	You can apply colors to value ranges for numbers, currencies, and counts on relationship fields. For information, see “Apply colors to value ranges” on page 408 .
Displaying alternate field labels	You can change the locale to display alternate field labels. For information, see “Applying alternate field labels” on page 405 .
Reviewing and associating related objects	You can add the ability to review and associate related objects, for example, a primary parent or child objects. For information, see “Adding a card layout” on page 414 and “Adding a grid layout” on page 425 .
Applying dynamic filters when associating related objects	You can apply dynamic filters when associating related objects using a card or grid relationship field. For information, see “Defining dynamic filters on actions in relationship fields” on page 438 .
Adding new objects	You can provide the ability to add new objects. For information, see “Adding actions to relationship fields” on page 434 .
Copying objects	You can provide the ability to copy objects. For information, see “Adding actions to relationship fields” on page 434 .
Adding files (attachments)	You can add the ability to add files (attachments). For information, see: • “Defining Task Views for file object types” on page 395 • “Defining Creation Views for file object types” on page 393
Delete objects	You can provide the ability to delete child objects. For information, see “Adding a Delete action” on page 438 .
Adding tree diagrams to display object relationships	You can display object relationships in a tree diagram. For information, see “Adding a tree diagram” on page 429 .
Adding charts to display object relationships	You can display object relationships in a chart diagram. For information, see “Adding a chart diagram” on page 416 .
Displaying related objects as a count	You can display related objects as a count. For information, see “Adding a count ” on page 424 .
Organizing relationship fields in tab groups.	“Organizing relationship fields in tab groups” on page 433

Table 149. Configurable UI components of a task view (continued)

UI component	Description
Accessing a natural language processing service	You can provide the ability to make suggestions using a natural language processing service. For information, see “Adding a classifier field that makes taxonomy suggestions” on page 410. For information, see “Adding a classifier field that makes object association suggestions” on page 430
Adding URL links	You can add URL fields that display as buttons or links. For information, see “Displaying a URL launcher field as a button or link” on page 410.

Using the View Designer

Use the View Designer to define, publish, and manage views in the Task Focused UI.

To open the View Designer, access the Task Focused UI and click  > **Solution Configuration** > **Views**. Your access permissions determine whether the menu item is displayed.

The View List is displayed.

View List

The View List shows views that are defined in the Task Focused UI. From the View List, you can:

- Click a view. The View Designer opens and you can view or make changes to the view.
- Select **Include system views** to show system views in the View List. The setting is cleared by default. Custom views are always listed.
- Click a column header to change the sort order of the list.
- Select the check box next to a single view or multiple views to update numerous views. The bulk update options are:
 - Delete
 - Enable
 - Disable

Clear the check boxes to hide the bulk update options.

- Click **Add New** to create a new view. After you define the initial properties, the View Designer opens. For more information, see:
 - [“Defining a Grid View”](#) on page 389
 - [“Defining a Creation View”](#) on page 391
 - [“Defining a Task View”](#) on page 394

The View Designer

The View Designer has the following components:

- **Design** tab
- **JSON** tab
- **Preview** tab

Design tab

The **Design** tab shows the definition of the view in a graphical format. It has the following components:

- Canvas

The canvas is where you lay out the view, create sections, and add fields to sections.

- Palette

UI components on the palette allow you to add inline guidance, groups, relationship fields, object fields, and workflow fields to a view. Use **Hide fields already in view** to control whether fields that are already added to the view are displayed in the palette.

- Property panel

The content of the property panel changes depending on what you select on the canvas. It can be properties that apply to a field or to a UI component (relationship field, group, inline guidance, and so on).

The following example shows the components on the **Design** tab:

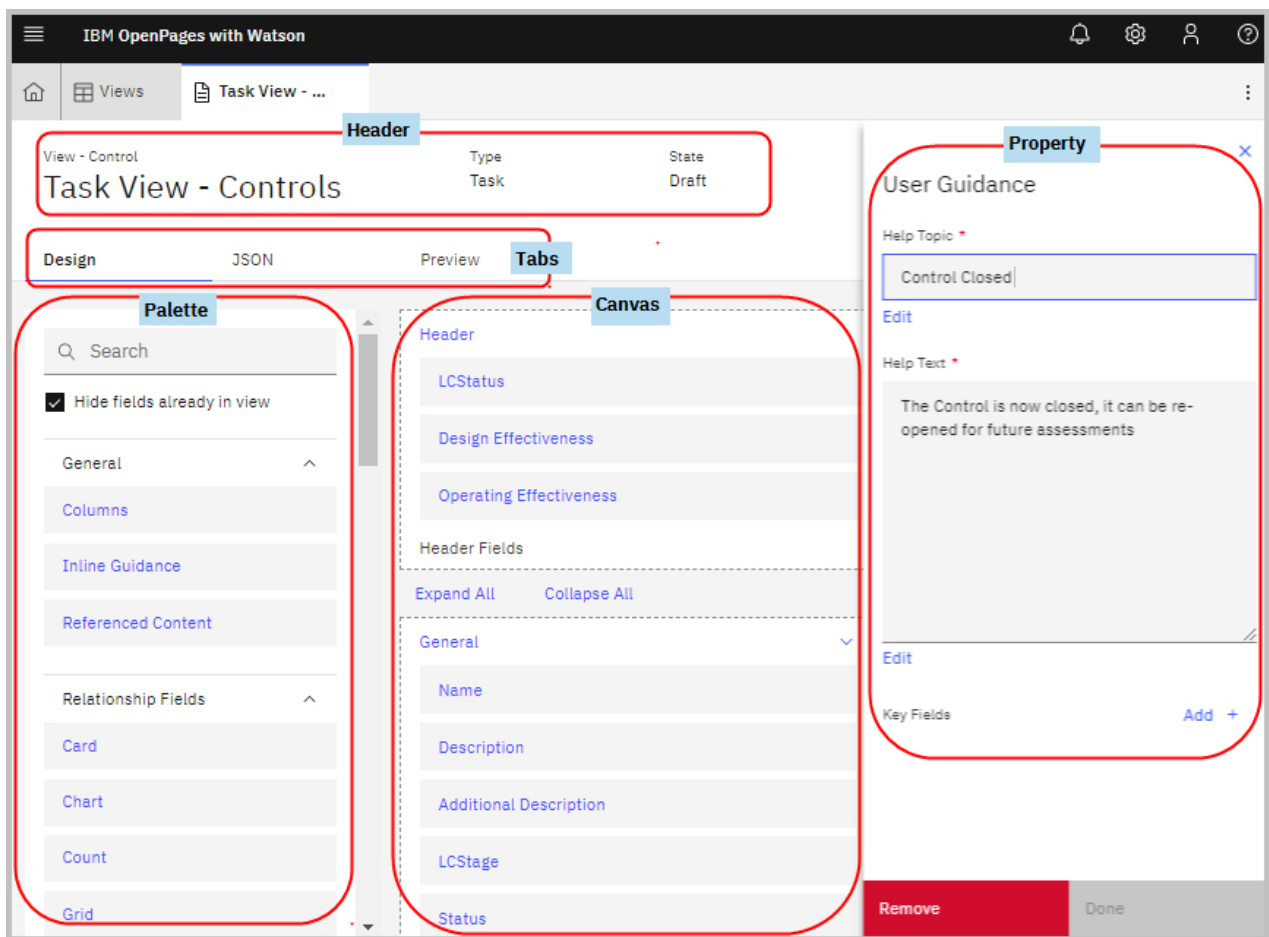


Figure 23. The Design tab in the View Designer

The **Design** tab is hidden for system views.

JSON tab

The JSON tab shows a view definition as JSON code.

The following example shows the JSON code for the previous task view definition.

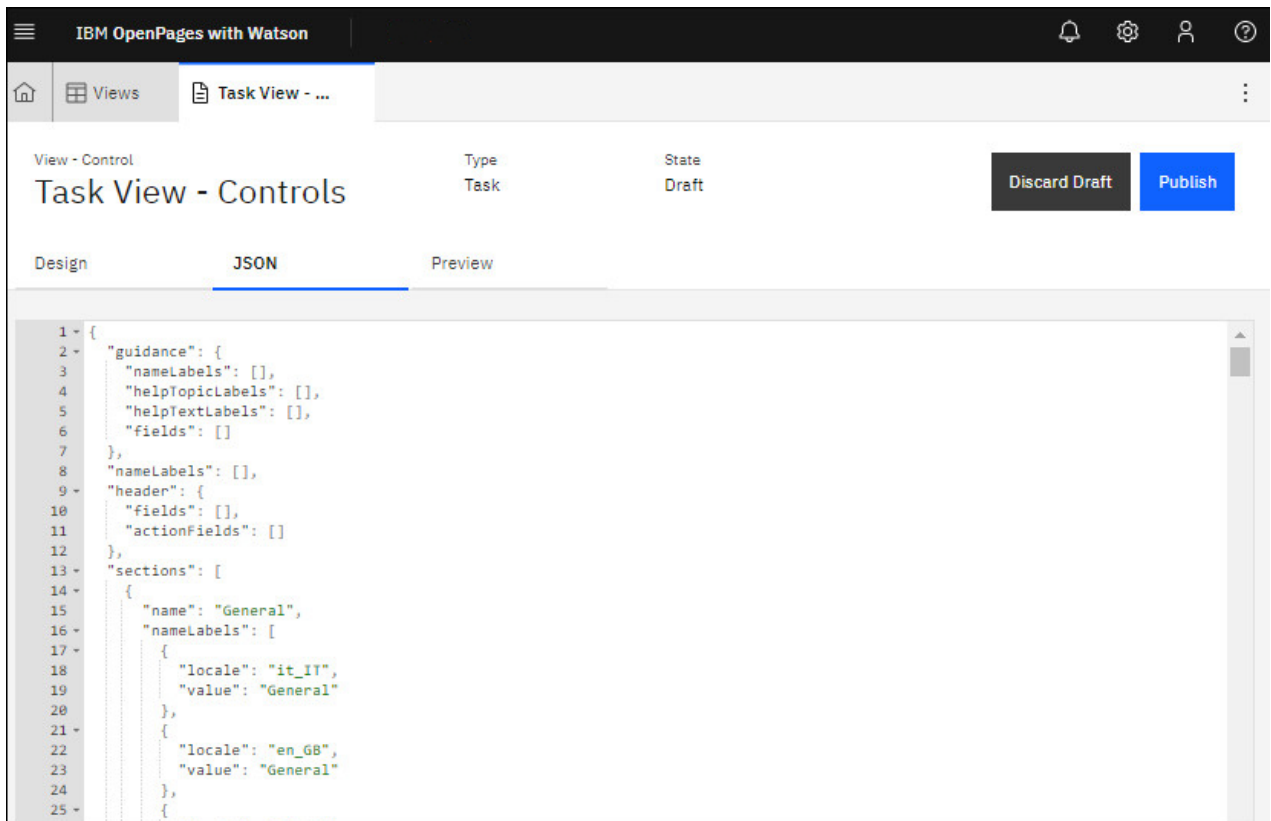


Figure 24. The JSON tab in the View Designer

For more information about JSON, see [“Editing JSON for a view definition” on page 398](#).

Preview tab

The **Preview** tab shows a view definition for an object instance. Up to 50 objects are displayed. Filters are disabled. Objects are read-only and cannot be changed. Workflow stages and workflow stage overrides are not considered. You cannot use the Preview tab to test how a view appears at different stages in a workflow and whether workflow task overrides are functioning correctly.

The following example shows the **Preview** tab for the previous task view definition.

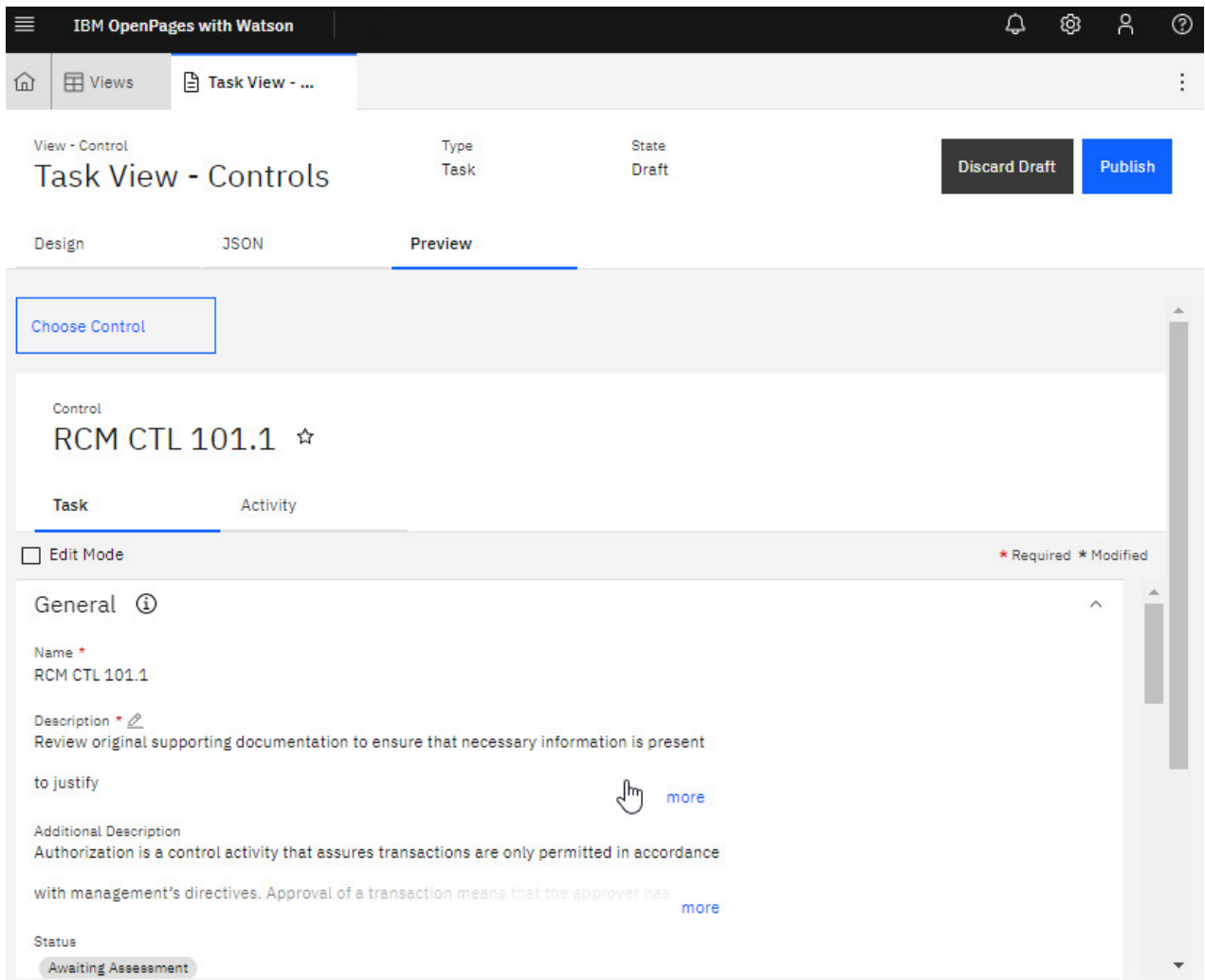


Figure 25. The Preview tab in the View Designer

Automatically translating labels

If it is configured, the [“IBM Watson Language Translator”](#) on page 1018 can help you define labels in multiple languages. There are numerous access points in the View Designer.

If it is displayed, click [Auto Translate](#)  to populate translated values to languages. For more information, see [“IBM Watson Language Translator”](#) on page 1018.

Saving a view

Your work is automatically saved as you edit a view. A general syntax validation check is performed every time that a view is saved.

Publishing a view

Click **Publish** when the view is finished. A detailed validation check is performed every time that a view is published. This validation check is more in depth than the one performed by the auto-save. It looks at whether the view is suitable for use and crosschecks the entire view. If you receive an error when you publish a view, you need to resolve it.

Discarding a draft version of a view

To discard changes you made to a view, click **Discard Draft**. All changes since the last published version are discarded.

Disabling a view

To disable a view, select a view from the list of views. Click the ellipse and then click **Edit**. Select **Disable**. Alternatively, in the View List, you can select a view and choose Disable in the bulk update options.

Working on a view as a team

When you have a view open in the View Designer, the URL contains the view's internal name. If you are working on the view with colleagues, you can send them the URL to share your progress. Although you can collaborate with colleagues, only one user should work on a view in the View Designer at a time.

Defining a Grid View

A Grid View definition contains basic information and rules. When used, a Grid View shows a list of objects for a selected object type and allows you to filter, search, select a specific object, and perform bulk updates on multiple objects.

Before you begin

Plan and design the Grid Views. For information, see [“Planning the Grid Views” on page 373](#).

If you define multiple Grid Views for an object type, see [“Controlling what views are displayed to users” on page 372](#).

Turn on the **Display debug info** feature. For information, see [“Displaying debug information” on page 397](#).

About this task

Each object type can have one or more Grid Views that are enabled.

For quicker system performance, apply a default filter to Grid Views that are defined for object types that potentially display a large number of objects.

Procedure

1. Click  > **Solution Configuration** > **Views**.
2. Click **Add New**.
3. Leave **Enabled** selected.
4. Select **Use as default view for this object type for all profiles** to make the view the default task view for the object type. If **Use as default view for this object type for all profiles** is cleared, you can click **Rules** and build the criteria that determines the Grid View that is displayed to a user.
5. Select an object type in **Object type**.
6. Enter a **Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
7. Select **Grid** in **View Type**.
8. Select a source view in **Copy from view (Optional)** to start with a base view that you can then modify. Choose a system Grid View, a published custom Grid View, or a Filtered List view from the Standard UI.

If you do not select a view, the new view is empty (minimum properties). You must design a new view.

9. Enter a **Description**.

10. If **Use as default view for this object type for all profiles** is cleared, you can click **Rules** and build the criteria that determines the Grid View that is displayed to a user.
11. Set **View Priority** to a numeric value, for example, 0, 1, or 2. It establishes the display priority of a Grid View compared to other Grid Views for the same object type. If multiple Grid Views match for a user after the rules have been checked, **View Priority** determines the view that is displayed to the user. A Grid View with the lowest value 0 is displayed first, then 1, then 2, and so on.
12. Optional: In **Profiles (if not specified, view is valid for all profiles)** select one or more profiles.
13. Click **Add**.
The View Designer opens with the **Design** tab displayed.
14. Design the view.
 - a) Set the **Bulk update** toggle to allow a field to be updated when a user clicks Bulk Update.
 - b) Add fields to the **Fields enabled for bulk update but not in grid view** section. Fields listed in this section are not displayed in the Grid View but users can update them when they click Bulk Update.See the following topics for configuration possibilities available for Grid Views:
 - [“Defining Grid Views for bulk workflow actions” on page 390](#)
 - [“Applying alternate field labels” on page 405](#)
 - [“Defining default filters on Grid Views” on page 406](#)
 - [“Apply colors to enumerated field values” on page 407](#)
 - [“Apply colors to value ranges” on page 408](#)
 - [“Displaying a number field as a progress bar” on page 410](#)
15. Click **Preview** to see how the view will appear to a user.
16. Click **Publish**.
17. Test the view. Each time you change the view, you need to publish it and re-test it.

What to do next

If you need to change the rules after a view is saved, click  and **Edit**.

Defining Grid Views for bulk workflow actions

Grid Views for bulk workflow actions are designed to optimized speed and efficiently as users work on actions created by GRC Workflow.

Before you begin

Understand the bulk workflow actions feature in GRC Workflow and determine whether it is needed.

Determine whether unique Grid Views are needed for the feature. Any Grid View can be used for bulk workflow actions. The reason to create unique Grid Views for bulk workflow actions is to customize the columns to meet the needs of the users completing the tasks.

About this task

A Grid View for bulk workflow actions is displayed when a user accesses tasks from the **Complete task with bulk workflow actions** window.

In the following example, a user selected to work with tasks assigned to them by the RCSA workflow, which is displayed in Workflow Name in the header. The stage is displayed next to the workflow name. In this example, the user has 43 risk assessments to review. The options in the toolbar, Approve, Reject, and Return, come from the workflow stage.

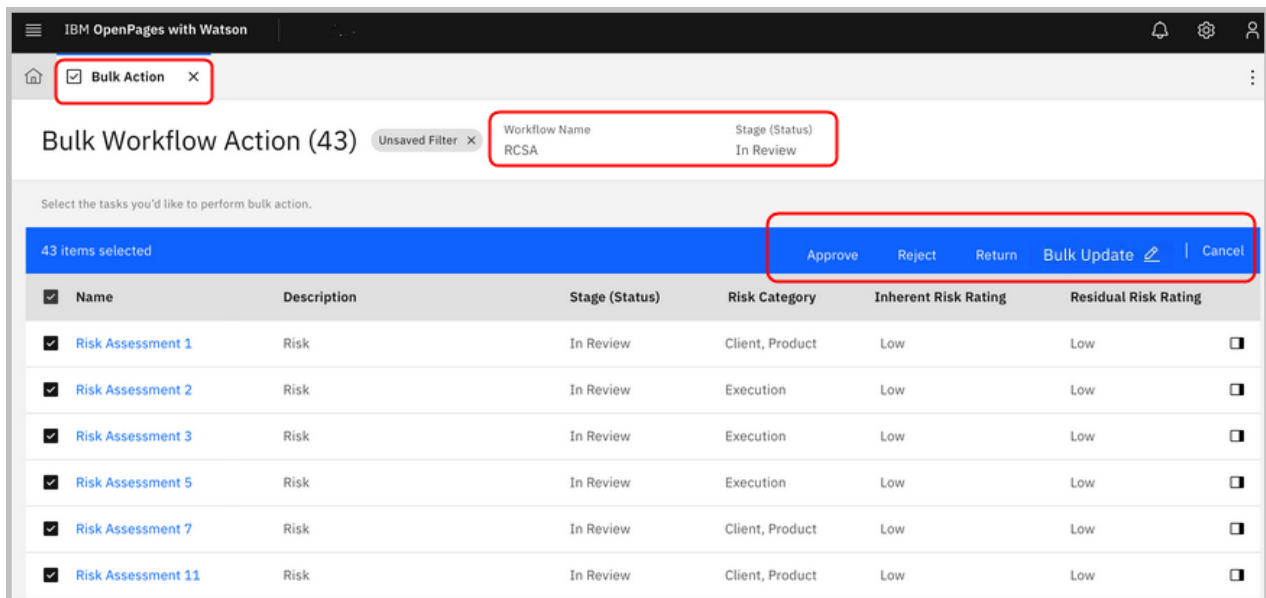


Figure 26. Example of a Grid View for bulk workflow actions

Functionality between a Grid View and Grid View for bulk workflow actions is mostly the same except for these differences:

- The Grid View that is displayed is defined in the workflow stage.
- The options in the toolbar are defined in the workflow stage. They cannot be configured in the View Designer.
- The **Add New** button is hidden.
- The tab name is always **Bulk Action**.
- The Grid View head is always Bulk Workflow Action.

Procedure

1. Follow the instructions in [“Defining a Grid View”](#) on page 389 to define a Grid View.
2. Add fields. The fields will be columns in the Grid View. Choose columns that will be helpful to the user when they work with bulk workflow actions.
3. Click **Done**.

What to do next

Add the Grid View to the workflow. Open the workflow and go to the **Bulk Workflow Action** section. Select the Grid View in **Select a grid view for Bulk Workflow Action**. For more information, see [“Defining a standard stage”](#) on page 519.

Defining a Creation View

A Creation View definition contains basic information and rules. When used, a Creation View enables a user to define new objects.

Before you begin

Plan and design the Creation Views. For information, see [“Planning the Creation Views”](#) on page 376.

If you define multiple Creation Views for an object type, see [“Controlling what views are displayed to users”](#) on page 372.

If you define Creation Views for file object types, see [“Defining Creation Views for file object types”](#) on page 393.

Turn on the **Display debug info** feature. For information, see [“Displaying debug information”](#) on page 397.

About this task

Each object type can have one or more Creation Views that are enabled.

Procedure

1. Click  > **Solution Configuration** > **Views**.
2. Click **Add New**.
3. Leave **Enabled** selected.
4. Select **Use as default view for this object type for all profiles** to make the view the default Creation View for the object type. If **Use as default view for this object type for all profiles** is cleared, you can click **Rules** and build the criteria that determines the Creation View that is displayed to a user.
5. Select an object type in **Object type**.
Do not choose File in **Object type**. To create files, use a relationship field. For information, see [“Defining Task Views for file object types”](#) on page 395.
6. Enter a **Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
7. Select **Creation** in **View Type**.
8. Select a source view in **Copy from view (Optional)** to start with a base view that you can then modify. Choose a system Creation View, a published custom Creation View, or a creation view from the Standard UI.
 - If you leave **Copy from view (Optional)** blank, the new view is empty (minimum properties). You must design a new view.
 - If you select **Detail**, the new view is set to the object type's detail view from the Standard UI. **Detail** is available only if there are no creation views in the Standard UI for the object type. Some object types do not have creation views in the Standard UI.
9. Enter a **Description**.
10. If **Use as default view for this object type for all profiles** is cleared, you can click **Rules** and build the criteria that determines the Creation View that is displayed to a user.
11. Set **View Priority** to a numeric value, for example, 0, 1, or 2. It establishes the display priority of a Creation View compared to other Creation Views for the same object type. If multiple Creation Views match for a user after the profile and parent object type rules have been checked, **View Priority** determines the view that is displayed to the user. A Creation View with the lowest value 0 is displayed first, then 1, then 2, and so on.
12. Optional: In **Profiles (if not specified, view is valid for all profiles)** select one or more profiles.
13. Optional: In **Parent Types (if known at creation time)** select one or more specific parent object types or **Any**.
If you use this rule, be sure you also have a default view that can be used if the parent object type is different than the selected object types, or if it is unknown at creation time. The parent object type is unknown, for example, when you click **Add New** from a Grid View or dashboard widget.
14. Click **Add**.
The View Designer opens with the **Design** tab displayed.
15. Design the view.

A Creation View must, at a minimum, contain a name. Depending on the object type, a primary parent might also be required, which you can add by using a card or grid relationship field that contains an action to associate a parent. For information, see [“Adding actions to relationship fields”](#) on page 434.

If you selected **Detail**, the new view contains fields from the object type's detail view that might not make sense in the context of object creation. Some fields from the object type's detail view may be excluded. Review the new view and make changes, if needed.

See topics in the following sections for all configuration possibilities available for Creation Views:

- [“Adding general elements to a view” on page 399](#)
- [“Adding and configuring fields on views” on page 407](#)
- [“Adding and configuring relationship fields on views” on page 413](#)
- [“Organizing relationship fields in tab groups” on page 433](#)
- [“Configuring rules” on page 439](#)

16. Click **Preview** to see how the view will appear to a user.

17. Click **Publish**.

18. Test the view. Each time you change the view, you need to publish it and re-test it.

What to do next

If you need to change the rules after a view is saved, click  and **Edit**.

Defining Creation Views for file object types

Creation Views are used to add files to the OpenPages file repository.

About this task

A Creation View for the File (SOXDocument) object type is used when users create new files from the following access points:

- A Task View that contains a grid relationship field for files. In this case, the parent object for the file is the object type of the Task View, for example, a Control or an Issue.

A **Files to add** window is shown after you select a file but before you click **Upload**. Creation Views for files determine the fields that are displayed in the **Files to add** pop-up window. Only required fields are displayed in the **Files to add** window.

- The  > **Attachments** > **Files** task. In this case, the parent object for the file is a business entity that the user provides. A **Files to add** window is not displayed.

When you plan Task Views that contain grid relationship fields for files, review the system Creation View for the File object type. You can use it as or create custom views if needed. It might be valuable to use multiple Creation Views for files so that you can control what displays in the **Files to add** pop-up window. You can define one Creation View for files and use it for all parent object types. Alternatively, define multiple Creation Views for files and use rules to control which Creation View for files is applied based on parent object type. Use the **Parent Types (if not specified, view is valid for all parent types)** rule on Creation Views to control what fields display in **Files to add**. For example, files that are added to a Policy object can include fields that support the Policy Import trigger. However, files that are uploaded to all other object types can exclude these fields. For more information, see [“Designing a Creation View” on page 377](#).

Creation Views are also used when users create files from the  > **Attachments** > **Files** task.

Creation Views are also used when administrators create new system files from the  > **System Configuration** > **System Files** task. System Creation Views are provided for the objects types for system files.

Procedure

1. Follow the instructions in [“Defining a Creation View” on page 391](#) to define a Creation View.

2. Select File in **Object type** (or one of the system file object types).
3. Add fields to the Creation View.
4. Drag a **File Uploader** element to a section. This element allows you to select a file to upload. It is unique to Creation Views for files. It is required.
5. Add a grid relationship field that contains an action to associate a parent. For more information, see [“Adding actions to relationship fields” on page 434](#). This is not applicable to Creation Views for system files.
6. Click **Done**.

Defining a Task View

A Task View definition contains basic information and rules. When used, a Task View enables a user to complete work that is assigned to them.

Before you begin

Plan and design the Task Views. For information, see [“Planning the Task Views” on page 380](#).

If you define multiple Task Views for an object type, see [“Controlling what views are displayed to users” on page 372](#).

If you define Task Views that allow users to add file attachments, see [“Defining Task Views for file object types” on page 395](#).

Turn on the **Display debug info** feature. For information, see [“Displaying debug information” on page 397](#).

About this task

Each object type can have one or more Task Views that are enabled.

Custom views can be edited. System views open in read-only mode and the **Design** tab is hidden.

Procedure

1. Click  > **Solution Configuration** > **Views**.
2. Click **Add New**.
3. Leave **Enabled** selected.
4. Select **Use as default view for this object type for all profiles** to make the view the default task view for the object type. If **Use as default view for this object type for all profiles** is cleared, you can click **Rules** and build the criteria that determines the Task View that is displayed to a user.
5. Select an object type in **Object type**.
6. Enter a **Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
7. Select **Task** in **View Type**.
8. Select a source view in **Copy from view (Optional)** to start with a base view that you can then modify. Choose a system Task View, a published custom Task View, or a Detail view from the Standard UI.
If you do not select a view to copy from, the new view is empty (minimum properties). You must design a new view.
9. Enter a **Description**.
10. If **Use as default view for this object type for all profiles** is cleared, you can click **Rules** and build the criteria that determines the Task View that is displayed to a user.
11. Set **View Priority** to a numeric value, for example, 0, 1, or 2. It establishes the display priority of a Task View compared to other Task Views for the same object type. If multiple Task Views match for a user after the profile, enumeration, and user rules have been checked, **View Priority** determines the

view that is displayed to the user. A Task View with the lowest value 0 is displayed first, then 1, then 2, and so on.

12. Set **Rule Operator** to one of the following options:

- **Logical AND of all rules**

All of the rules (profile, enumeration rules, and user rules) must be met for the view to be shown to a user.

- **Logical OR of all rules**

Any one of the rules (profile, enumeration rules, and user rules) must be met for the view to be shown to a user.

13. Optional: In **Profiles (if not specified, view is valid for all profiles)** select one or more profiles.

14. In **Enumeration rule** you can set a view to display if the value of an enumeration field on the object is a specific value.

a) In **Rule Field** select the field that the rule is based on.

b) In **Rule Condition** select the condition, for example, equal (=) or not equal to (<>).

c) In **Rule Value** select the value that the rule tests against.

d) Click **Enumeration Rule**  to add more enumeration rules.

15. In **User rule** you can set a view to display if the signed on user has the role of the value selected, for example, is the owner or assignee of the object.

a) In **Rule Field** select the field that the rule is based on, for example, assignee or <object> owner.

b) Click **User Rule**  to add more user rules.

16. Click **Add**.

The View Designer opens with the **Design** tab displayed.

17. Design the view.

See topics in the following sections for all configuration possibilities available for Task Views:

- [“Adding general elements to a view” on page 399](#)
- [“Adding and configuring fields on views” on page 407](#)
- [“Adding and configuring relationship fields on views” on page 413](#)
- [“Organizing relationship fields in tab groups” on page 433](#)
- [“Configuring rules” on page 439](#)

18. Click **Preview** to review the view.

19. Click **Publish**.

20. Test the view. Each time you change the view or the rules, you need to publish it and re-test it.

What to do next

If you need to change the rules after a view is saved, click  and **Edit**.

Defining Task Views for file object types

To support adding and managing files (attachments) in Task Views, define a Task View for the File (SOXDocument) object type.

Before you begin

Complete the following prerequisites:

- Define Task Views for object types, for example, Controls and Issues, that allow file attachments. Add a grid relationship field where **Object Type** is set to File and **Relationship Type** is set to children. The **Add/Update** button automatically displays in a grid relationship field. It is used to upload new files to the selected object. If you add an Association action, users can also associate files that are already uploaded to other objects. They can also disassociate files by selecting a row and clicking **Remove**.
- Review the Creation Views for the File (SOXDocument) object type. A Creation View for files is required to add file attachments in a Task View. Use the system view for the File object type as is or create custom views. For more information, see [“Defining Creation Views for file object types”](#) on page 393.
- Configure whether Microsoft Office documents can be opened and edited directly from OpenPages. For more information, see [“Allow opening Microsoft Office files directly from OpenPages”](#) on page 617.

About this task

In the following example, a Task View for Audit objects contains a grid relationship field for files. An Audit object is open and you can upload a file by clicking **Add/Update** or dragging a file to the Task View. You can also click **Associate action** to associate an existing file to the object and **Remove** to disassociate objects.

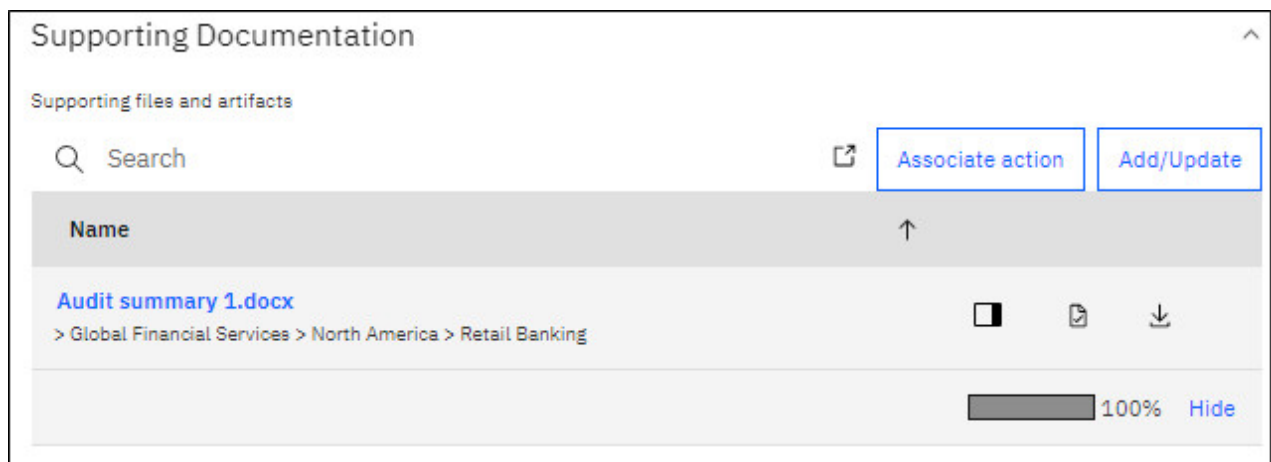


Figure 27. Example of a Task View for files

For more information about relationship fields, see [“Adding a grid layout”](#) on page 425.

In addition to having a relationship field for files in a Task View, you must also define Task Views for the File object type. When you click a file name in a grid relationship field for files, the Task View for the File object type opens.

Define one Task View for the File object type and use it for all parent object types. Alternatively, define multiple Task Views for the File object type and use rules to control which Task View for files is displayed for each parent object type.

OpenPages uses version control and file locking in the file repository. When you work in a collaborative team environment, files are checked in and out to ensure that changes made by one team member will not be overwritten by another team member.

Version management and the ability to check in and check out files are always enabled. The check in and check out icons require no configuration. You can, however, control whether a **Versions** element in a Task View for files is displayed. It allows you to view and work with multiple versions of a file.

In this example, the Task View for the Files object type is defined with File Name, Description, Document Type, Folder, Active, Last Modification Date, and a Versions element.

File
Audit summary 1.docx
Print
Check Out

Task
Activity

☐ Edit Mode
* Required * Modified

General ⓘ

Name *
Audit summary 1.docx

Description

Created By *
System Administrator - OpenPagesAdministrator

Creation Date *
Mar 31, 2020 12:31:57 PM GMT

Last Modified By *
System Administrator - OpenPagesAdministrator

Last Modification Date *
Mar 31, 2020 12:31:57 PM GMT

Folder *
/ Global Financial Services / North America / Retail Banking

Versions

Search
Update

Last Modification Date	↑	Last Modified By	↑	Comment	↑
Mar 31, 2020 12:31:57 PM GMT		System Administrator - OpenPagesAdministrator			

Figure 28. Example of a Task View for files

Task Views are also used when users view files from the  > **Attachments** > **Files** task.

Task Views are also used when administrators view system files from the  > **System Configuration** > **System Files** task. System Task Views are provided for the objects types for system files.

Procedure

1. Follow the instructions in “Defining a Task View” on page 394 to define a Task View.
2. Select File in **Object type** (or one of the system file object types).
3. Add fields to the Task View.
4. Drag a **Versions** element to a section. This element allows you to view and manage multiple versions of a file. It is unique to Task Views for files.
 - a) Apply rules to the Versions element (optional). For more information, see “Configuring rules” on page 439.
 - b) Click **Done**.
5. Click **Done**.

Displaying debug information

Use **Display debug info** to turn on debug mode and resolve problems as you configure views.

About this task

When **Display debug info** is enabled, the following additional elements are displayed in the header when you access views:

- The name of the view that is open.

When the view name is shown, you can test the view rules and verify that the correct view is displayed. Click the view name, and the View Designer opens.

- **Why can't I save?**

Why can't I save? is displayed in Task Views and Creation Views if there's a problem that prevents you from saving your work. For example, if a required field for an object is empty, the **Save** button is disabled. Click **Why can't I save?** to view informational text that explains why **Save** is not enabled.

Procedure

1. Click  > **Other** > **Display Debug Info**.
Debug mode is turned on and a check mark displays next to **Display Debug Info**.
2. To turn off debug mode, click **Display debug info** again.
Debug mode is turned off and the check mark is removed.

Creating a custom view from a system view

You can create a custom view by making a copy of a system or custom view and modifying the new view.

Before you begin

The source view and the new custom view must be for the same view type and the same object type, for example, both views must be task views for Issues.

About this task

Copy all the JSON code for the view you want to copy. Although you can copy only snippets, errors will occur if the snippet is not precisely placed in the JSON code in the new view.

For system views, in the View Designer you can view the **JSON** tab but the **Design** tab is hidden. To view a system view in the **Design** tab, copy it to a custom view and open the **Design** tab in the custom view.

Procedure

1. Click  > **Solution Configuration** > **Views**.
2. On the list of views, click **Include system views**.
3. Select the system or custom view that you want to use as the source.
4. Click **JSON**.
5. Select all the JSON code to put it on your clipboard.
6. Go back to the list of views and click **Add New**.
7. Define basic information for the new view.
8. Click the **JSON** tab in the new view, delete the existing JSON code and paste the JSON code that is on the clipboard.
9. Click **Design**.
The JSON code from the source view is rendered on the **Design** tab.
10. Remain on the **Design** tab and begin making changes to the new custom view. You do not have to edit the JSON to make changes to the new view. Changes you make on the **Design** tab are automatically made in the JSON.

Editing JSON for a view definition

The content and layout of views is defined in JSON, which is syntax for defining structured data.

When to use the JSON tab

Use the **JSON** tab to copy views. For more information, see [“Creating a custom view from a system view” on page 398](#).

Other than copying views, there is no need to use the **JSON** tab. You can optionally check how a view is structured and search for JSON property and element names. You can solely use the **Design** tab to create and design custom views. All the capabilities in the **JSON** tab are also in the **Design** tab.

Tips for fixing JSON mistakes

The JSON editor checks syntax and shows mistakes.

- The mistake is usually in the line just before the line with a red x.
- Check first for mismatched delimiters (curly braces and square brackets) and trailing commas. They are the most common mistakes. The error message might not clearly state that the problem is a delimiter.

Tips for copying JSON and minimizing copy errors

Avoid errors by copying an entire view rather than JSON snippets.

If you copy a JSON snippet, use the small triangles in the left gutter to collapse the JSON before you select a JSON snippet. When the text is collapsed, it is easier for you to select what you want to copy.

Before you paste a JSON snippet, collapse the area that you are pasting into so that it is easier to identify the correct insertion point.

Adding general elements to a view

You can control a view's fundamental content and organization.

Adding a section

Information in a view definition is organized into sections.

About this task

Sections are valid in Creation Views and Task Views.

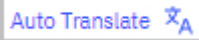
A section contains fields and, optionally, inline guidance. When you work on the **Design** tab:

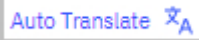
- You can control the order of sections in a view.
- You can define whether a section is collapsed or expanded when a user initially opens a view.
- You can expand and collapse individual sections and also use the **Expand All** and **Collapse All** toggles.
- You cannot embed a section in another section.
- You can add fields directly to sections, in which case they are ordered consecutively down the page in the view.
- You can add groups to sections and then add fields to groups, in which case you can arrange the fields in columns and place them more precisely in the view.
- If a Task View is used in a workflow, task view overrides can hide a section and override the **Initially Collapsed** setting. For information see, [“Defining a standard stage” on page 519](#).

On the JSON tab, a section is defined in a `sections` element.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Click **Add Section**, which is always displayed as the last section.
3. Enter a **Label**. It displays as the section header. Click **Edit** to enter localized values.



If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

4. Set **Initially Collapsed** to True or False.
5. Click **Done**.
6. Expand the new section and start adding fields and groups.
 - a) To add a field directly to the section, drag it into **Section Fields**.
 - You can drag a field either from the palette or the canvas and drop it into the section.
 - You can change the order of fields in a section.
 - b) To add groups, see [“Arranging fields in columns” on page 400](#).
7. Drag an **Inline Guidance** element from the palette to the section (optional). For information, see [“Adding inline guidance” on page 400](#).
8. Click **Done**.
9. Move the section up or down to change the display order.

Arranging fields in columns

You can use columns (groups) to control field placement in a view.

About this task

Columns are valid in Creation Views and Task Views.

When you work on the **Design** tab:

- A group must be within a section.
- Groups can contain object fields and relationship fields.
- A group cannot be embedded in another group.

If multiple columns are defined but horizontal space is limited, the display changes to a single column.

You can find an example in: SysView-Task-SOXControl.

On the JSON tab, columns are defined in a `columns` property.

Procedure

1. In the View Designer, click the **Design** tab.

The palette is displayed.
2. Drag a **Column** element from the palette to the section where you want it to display.
3. Enter a value in **Name**. This is an internal name that is not displayed in the view.
4. Select a number in **Number of Columns**. You can define no more than four columns.
5. Click **Done**.
6. Add fields to the group. You can drag a field either from the palette or the canvas and drop it into **Group Fields**.
7. Move fields up or down to change the display order.

Adding inline guidance

Inline guidance displays customer-specific help text that supports users as they complete a task. It is displayed as a field and enclosed in a box.

About this task

Inline guidance is valid in Creation Views and Task Views.

Each section can contain one or more inline guidance elements.

Visible or hidden rules can be applied to each field within an inline guidance section.

When it is displayed in a view, users can expand or collapse the text if it is long.

IBM OpenPages with Watson

Workflows Issue Review... Business Ent... + *New Loss E...

Loss Event

New Loss Event

Cancel Save

* Required * Modified

General

Name *

_LE_0002

*Description *

Stolen customer data

*Owner *

orm

Search users

*Outcome

Loss

*What Happened

A missing security patch allowed hackers to enter the server hosting the online banking system. System was brought down for several hours while the problem was corrected.

Inline guidance

Please provide correction information based on the information provided by the responsible parties.

Figure 29. Example of inline guidance

On the JSON tab, inline help is defined in *helpTopic* and *helpText* properties.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag an **Inline Guidance** element from the palette to a section.

3. Enter a value in **Name**. This is an internal name that is not displayed in the view.
4. Enter text in **Help Topic**. This value is displayed in bold as a header. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

5. Enter text in **Help Text**. This value is the informational text to which you can optionally apply formatting. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

6. Add a hidden or visible rule (optional). For information, see [“Defining Visible and Hidden rules” on page 441](#).
7. Optional: Apply formatting. For more information, see [“Applying light formatting to text ” on page 403](#).
8. Click **Done**.

Adding user guidance

User guidance supports users as they complete a task and resolve issues.

About this task

User guidance is valid in Creation Views and Task Views.

User guidance is displayed in a panel in the upper right corner of a view. It contains informational text, a progress bar, and a list of key items. If a task is part of a workflow that has started, **Select an action to validate** is also displayed. Messages and field symbols guide users through finishing a task.

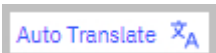
When it is displayed in a view, users can expand or collapse the text if it is long.

A view can have one user guidance section. The name *user guidance* is shown in the View Designer but the section has no title when it is displayed in a view.

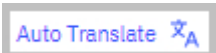
For more information about user guidance, see [“How key items and workflow actions display in user guidance ” on page 403](#).

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Click **User Guidance**. The User Guidance panel opens.
3. Enter text in **Help Topic**. This value is displayed in bold as a header. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

4. Enter text in **Help Text**. This value is the informational text to which you can optionally apply formatting. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

5. Build the list of key fields. There are two methods. For object fields, you can follow this method:
 - a) In the User Guidance panel, click **Add**. A list of object fields is displayed.
 - b) Tick the fields that you want to include as key fields.
 - c) Move key items up and down to change the display order.
 - d) Click **Done**. The User Guidance panel closes. The panel changes to a list of key fields.

For object fields and any other fields, for example, relationship fields, that are on the canvas, follow this method:

- a) Close the User Guidance panel if it is open.
- b) Drag fields from the canvas to the list of key fields. A field can be dropped when the list of key fields is framed with a blue box. If the field does not drop, it is already marked as a key field.
- c) Move key items up and down to change the display order.

You do not have to add required fields as key items. However, if you add them, you can control the display order.

6. Optional: Apply formatting. For more information, see [“Applying light formatting to text ” on page 403.](#)

How key items and workflow actions display in user guidance

You can configure key items and how they are ordered in user guidance.

Key items in user guidance

Key items are listed after the informational text under the title **Key Items**. You configure the list of key items. In addition, required fields and invalid fields are automatically listed as key items. When a user clicks a key item, the cursor moves to that field and places it in edit mode. The symbols next to a field indicate its status. The symbols are fixed and cannot be changed.

Workflow actions and user guidance

If a task is part of a workflow that has started, **Select an action to validate** is displayed in the user guidance panel.

For more information about defining validations on actions, see [“Defining a workflow action” on page 527.](#)

The workflow information card appears above the user guidance and contains summary information.

Neither **Select an action to validate** nor the workflow information card requires configuration.

Task view overrides can change the user guidance and key items that are displayed. For information, see [“Defining a standard stage” on page 519.](#)

See the *IBM OpenPages with Watson User Guide* for more information about how users work with the user guidance panel.

Applying light formatting to text

You can apply light formatting to text in inline guidance, user guidance, and object text for field guidance.

About this task

HTML and line breaks are not supported.

Procedure

1. Access a task where you can define text, for example, defining inline guidance for a Task View in the View Designer.
2. Apply the following formatting to text:
 - To apply italics, enclose text in single asterisks, for example, **text**.
 - To apply bold, enclose text in double asterisks, for example, ****text****.
 - To insert a hyperlink, provide a fully qualified URL. For example, <https://www.ibm.com> displays in a view as a hyperlink named **https://www.ibm.com**.
 - To insert a hyperlink as a link title, provide it in the [Link title] (URL) format. For example, <https://www.ibm.com> displays in a view as a hyperlink named **https://www.ibm.com**.

- To begin a new paragraph, press enter twice.
 - To format text as a bulleted item, enter - (hyphen followed by one space and text) or * (asterisk followed by one space and text).
 - To apply a heading level one, begin the text with `##` followed by a space, for example, `## This is a Heading One`. Use `###` for heading level two, and so on. The maximum is six heading levels.
3. Alternatively, for inline guidance and user guidance on the JSON tab:
- Press enter to begin a new line (indented).
 - `\n*` (`\n*` followed by one space and text) formats text as a bulleted item.
 - `\n\n` begins a new paragraph.

Defining a Task View header

A Task View header contains object information and, optionally, an **Actions** button and fields.

About this task

A task view header is valid only in Task Views.

You can add an **Actions** button and up to three fields to a Task View header, where the field type can be integer, decimal, currency, simple text, enumerated, user, date, and relationship count. The Task View header has limited space so add fields whose content is short and concise.

If the object type has workflows, the workflow drives the options on the **Actions** button. For information, see [“How users interact with workflows” on page 499](#).

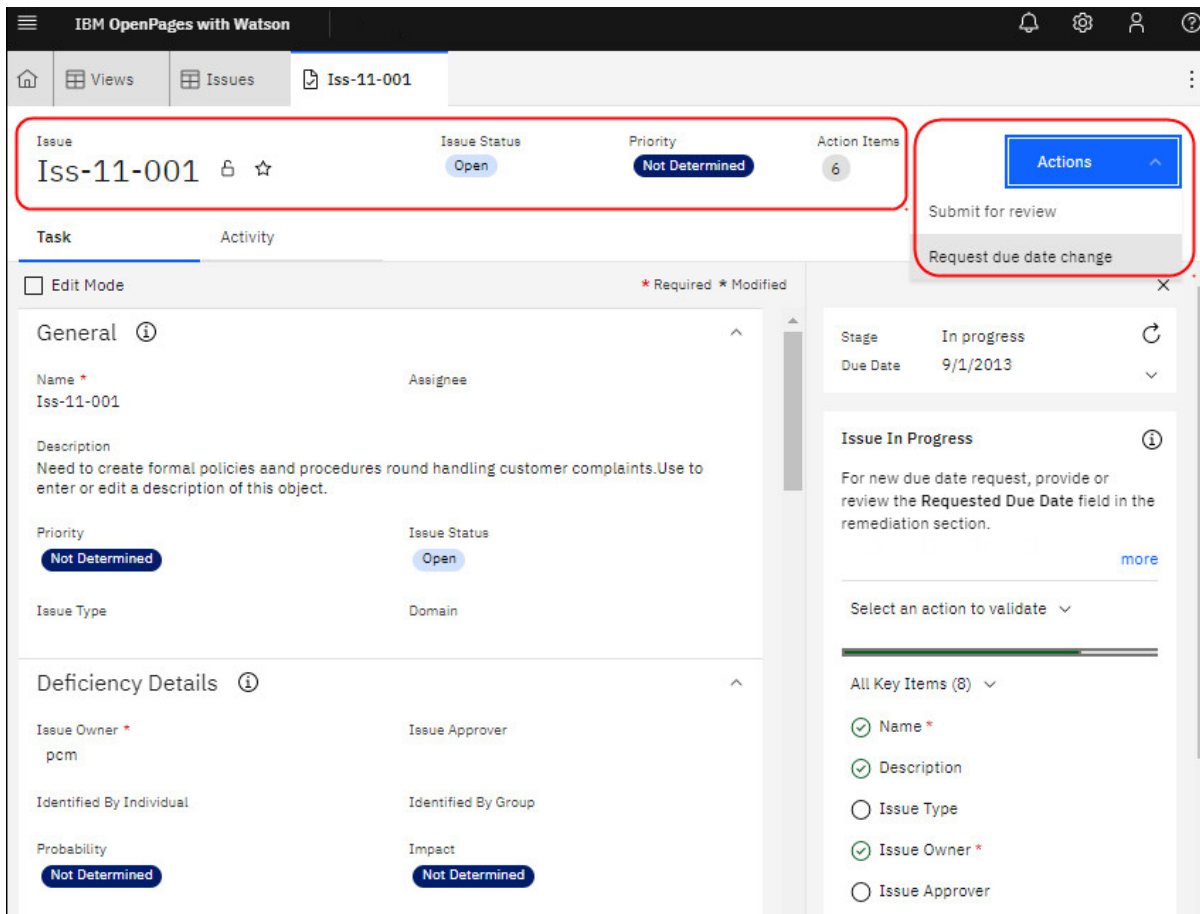
The options on the **Actions** button can be configured to allow a user to enter a comment. The comment can be required or optional. For information, see [“Defining a workflow action” on page 527](#).

If the object type does not have workflows, you can add one **Actions** button. The actions facilitate moving the object to the next stage in its lifecycle. The values are from any set of enumerated field values or from the configurable lifecycle transitions for the object. The field type must be enumerated. The label of the **Actions** button is fixed and cannot be changed.

You cannot add rules to fields in the Task View header.

In this example, the Task View header for the Issue object contains three fields: Issue Status, Priority, and Action Items.

Figure 30. Example of a Task View header for issues



You can find an example in: SysView-Task-SOXIssue.

On the JSON tab, a task view header is defined in a *header* element.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Expand the **Header** panel.
3. In **Lifecycle Action**, choose an enumerated field that drives the **Actions** button.
4. Add fields to the header. You can drag a field either from the palette or the canvas and drop it into the group.

Applying alternate field labels

You can apply alternate field labels to support localization.

About this task

Alternate field labels are valid in Grid Views, Creation Views, and Task Views.

You can apply labels to fields and UI components in the Task Focused UI that do not have localized text that is defined in the Standard UI. The names of sections, inline guidances, and relationship fields are unique to the Task Focused UI and have no localized text until you create it. For example, a section that is titled Remediation in English has no translated string in German. When you add the German title, a string key is automatically created.

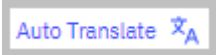
For information about localization, see Chapter 17, “Localizing text,” on page 559.

You can provide localized text only for labels where an **Edit** button is displayed.

On the JSON tab, localized values are defined in `nameLabels` properties for fields and UI components.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the UI component, for example, a relationship field or a section.
3. Enter a value in the label. The value you entered is populated to all languages.
4. Click **Edit**.
5. Enter localized text for one or more languages.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

6. Click **Done**.

Results

String keys are automatically created for the localized text you add. If values change in the future, repeat the steps and make the changes.

Defining default filters on Grid Views

You can add default filter rules to a Grid View.

About this task

If you define a default filter, a check box with the label you provide displays at the top of the grid. It is selected by default. Only objects that match the filter are displayed in a view.

For quicker system performance, apply a default filter to Grid Views that are defined for object types that potentially display a large number of objects.

Filters can be based only on single value enumerated fields. A Grid View can have only one default filter but it can have multiple rules. An object must meet all rules to match the filter.

Grid Views for object types that have workflows display a filter named **Active Only**. If you define a default filter rule for an object type that has workflows, it overwrites the **Active Only** filter.

An example of a default filter is that you want a Grid View for SOXRisk objects to display only objects whose Status field is set to Approved. A check box labeled **Only display approved items** is displayed at the top of the grid.

You can use a filter so that a Grid View for SOXRisk objects displays only objects whose Status field is set to Reject and whose Audit Inherent Impact is 1 or 2. One check box labeled **Only display rejected items** is displayed at the top of the grid.

For more information about rules, see [“Configuring rules” on page 439](#).

On the JSON tab, default filter rules are defined in a `defaultFilterRules` element in a Grid View.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. On the canvas, click **Define default filter**.
3. Specify a **Label**. This name displays at the top of the grid.
4. Click **Add Rule**.

5. In **Field**, choose the field that the filter is based on. Only single value enumerated fields are listed.
6. In **Matches any of**, select the value or values that you want to filter on. If you add multiple values, an object must have one of the values to match the filter.
7. Click **Done**.
8. Add more rules, if needed. If you add multiple rules, an object must meet all rules to match the filter.
9. Click **Done**.

What to do next

Publish the Grid View to test the filter. Filters are not supported on the **Preview** tab.

Adding and configuring fields on views

You can apply colors to fields, control display, and add different kinds of fields to views.

Apply colors to enumerated field values

You can apply colors to enumerated field values.

About this task

Colors can be applied to enumerated fields in Grid Views, Creation Views, and Task Views.

Colors are saved at the field level. Colors for enumerated field values are displayed in all published custom views that contain the field. If a color for an enumerated field value is defined in multiple views, changing a color in one view changes it in all views, including system views. The colors defined in the last published custom view take precedence.

For a list of color values, see [“Supported color palettes for field values”](#) on page 409.

In the following example, color is applied to values for the Inherent Risk Rating and Residual Risk Rating fields. Note that High, Low, and Very High are enumerated string values, not translated labels.

Figure 31. Example of colors applies to enumerated value fields



You can find an example in: SysView-Task-SOXRisk.

On the JSON tab, colors for enumerated field values are defined in an `enumValueColors` element.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. On the canvas, click an enumerated field. The field attribute panel opens.
3. Choose Categorical or Monochromatic in **Color Palette**.
4. In **Color Values**, choose a color for each enumerated value for the field. The available colors depend on the color palette you selected.
If you choose no color (the white cell), the value renders as gray.
5. Click **Done**.
6. Publish the view for the color to take effect in all custom views that contain the field.

Apply colors to value ranges

You can apply colors to value ranges for numbers, currencies, progress bars, and counts.

About this task

Color ranges are valid in Grid Views, Creation Views, and Task Views.

Color ranges are saved at the field level. Color ranges are displayed in all published custom views that contain the field. If a color range is defined in multiple views, changing a color range in one view changes it in all views, including system views. The color range defined in the last published custom view takes precedence.

For a list of color values, see [“Supported color palettes for field values”](#) on page 409.

For currencies, the color that is applied is based on the base currency. For example, if the local amount is 20 EUR and the base currency is USD and the exchange rate is 2, the applied color is based on 40 USD.

When you build color ranges, the following rules apply:

- Overlaps in range values are not allowed.
- If you choose no color (the white cell), the value renders as gray.
- For object fields, the initial minimum and maximum values that are displayed in a color range come from the field definition. If a field has no minimum or maximum in its field definition, negative infinity is used as its minimum value and infinity is used as its maximum value.
- For count-based relationship fields, the minimum is always zero and the maximum is infinity (count fields have no field definitions from which to get minimum and maximum values).
- A typical definition of a color range has no gaps in the range values, and the top value of one range is equal to the bottom value of the next range.
- If there are gaps in ranges, the value renders as gray.
- In general, the bottom value in a range is inclusive and the top value is exclusive. This enables the system to correctly apply colors to decimal values. An exception exists for the top value of the highest possible range, which is always inclusive so that a color is applied to the maximum value of a field.

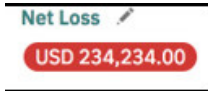
The following example shows how colors are rendered for a typical color range.

Table 150. Example for a field that has a maximum value of 100		
Range	Color	Result
0-25	Green	0 and all values up to but not including 25 display as green.
25-50	Yellow	25 and all values up to but not including 50 display as yellow.
50-100	Red	50 and all values up to and including 100 display as red.

If the same field had a maximum value of infinity, the colors are applied as follows:

Table 151. Example for a field that has no defined maximum value		
Range	Color	Result
0-25	Green	0 and all values up to but not including 25 display as green.
25-50	Yellow	25 and all values up to but not including 50 display as yellow.

Table 151. Example for a field that has no defined maximum value (continued)		
Range	Color	Result
50-100	Red	50 and all values up to but not including 100 display as red.
100 to infinity	Dark Red	100 and all values above 100 display as dark red.



On the JSON tab, color ranges are defined in a *numberRangeColors* element.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. On the canvas, click the field to which you want to apply a color range. The field attribute panel opens.
3. In **Color Ranges**, click  to start building ranges.
4. Click **Done**.
5. Publish the view for the color range to take effect in all custom views that contain the field.

Supported color palettes for field values

Available colors for field values are based on two Carbon color palettes, Categorical and Monochromatic.

When you apply colors to enumerated fields and fields in charts, colors can be chosen from either the Categorical or the Monochromatic palette. The palettes have been designed to be aesthetically inviting for users. They also maximize contrast between the background color and the colors of the UI elements so that they are compliant with accessibility standards.

The Categorical palette has a light and dark set of colors, which are based on the light and dark themes. When you are defining views and charts, the theme that is applied to the signed on user determines the colors that are available in the categorical palette. If the signed on user is using a light theme, the light color set in the Categorical palette is displayed. If the signed on user is using a dark theme, the dark color set in the Categorical palette is displayed.

How colors display to a user depends on the theme that they're using. The system finds the closest match between how the field or chart was defined and how the theme is defined.

In previous versions, a fixed list of colors was supported. The system finds the closest match between those colors and the Carbon palette colors. Fields must not be redefined. However, you might want to review your field colors and take advantage of the palettes to improve the system to be more visually aesthetic and to meet accessibility standards.

For more information about applying colors, see [“Apply colors to value ranges” on page 408](#) and [“Apply colors to enumerated field values” on page 407](#).

For more information about themes, see [“Themes” on page 452](#).

For more information about the palettes, see the following Carbon documentation:

- <https://www.carbondesignsystem.com/data-visualization/color-palettes/>
- <https://www.carbondesignsystem.com/guidelines/color/usage/>

Design tab

On the **Design** tab, if you choose no color (the white cell), the value renders as transparent.

JSON tab

On the JSON tab, a color is defined in a *color* property.

Displaying a URL launcher field as a button or link

You can configure a URL launcher field to display as a button or link.

About this task

The property that controls how a URL launcher field is displayed is valid in Creation Views and Task Views.

URL launcher fields can be configured as a button or link. Whereas, URL fields always display as links.

Display Type is not shown in the property panel for URL fields.

For more information about URL launcher fields, see [“Using object fields to launch JavaServer Pages and external URLs”](#) on page 244.

On the JSON tab, display type is defined by setting *subDisplayType* to `button` or `link`. The field's display type must be set to URL. If *subDisplayType* is not provided, the URL field displays as a link.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Click a URL launcher field.
3. In the properties panel, set **Display Type** to **Button** or **Link**.

Displaying a number field as a progress bar

You can display a number field as a progress bar. Valid in Grid Views, Creation Views, and Task Views.

About this task

You can configure a number field to display as a progress bar. The field must be an integer or decimal, and it must have a minimum and maximum value that is defined at the field level.

For information about defining color ranges, see [“Apply colors to value ranges”](#) on page 408.

On the JSON tab, a progress bar is defined by setting *subDisplayType* to `Progress` for a number field.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Click the field that you want to display as a progress bar.
3. In the properties panel, set **Display Type** to **Progress**.
4. Click **Done**.

Adding a classifier field that makes taxonomy suggestions

You can add classifier fields that make taxonomy suggestions using a natural language processing service.

Before you begin

The natural language processing service must already be configured to make taxonomy suggestions. Find out the classifier fields and classifier target fields before you get started. For information, see [“Natural language processing services”](#) on page 1021.

About this task

Classifier fields that make taxonomy suggestions are valid in Creation Views and Task Views.

The Task Focused UI supports making taxonomy suggestions and object association suggestions. For information about object association suggestions, see [“Adding a classifier field that makes object association suggestions”](#) on page 430.

When a user accesses a Creation View or Task View with a classifier field, an IBM Watson Insights button appears in place of the classifier field. The button name changes to the classifier field label. Click the button and an IBM Watson Insights panel displays the results.

The classifier field and the classifier input field must both be in the view. The classifier target fields can optionally be included in the view. It is not necessary to configure the Watson statement on the classifier input field (*Adding a description improves IBM Watson Suggestions*), the IBM Watson Insights button, or the IBM Watson Insights panel. These elements display automatically for classifier fields.

The classifier field label is used as both the button label and the title of the IBM Watson Insights panel. Otherwise, they cannot be customized.

You can add multiple classifier fields to a view.

You can not add classifier fields that make taxonomy suggestions to Grid Views. You can, however, add classifier target fields to Grid Views.

In this example, the text in the Description is used as input to a natural language processing service that makes taxonomy suggestions. The loss event categorization field is configured to be a classifier field.

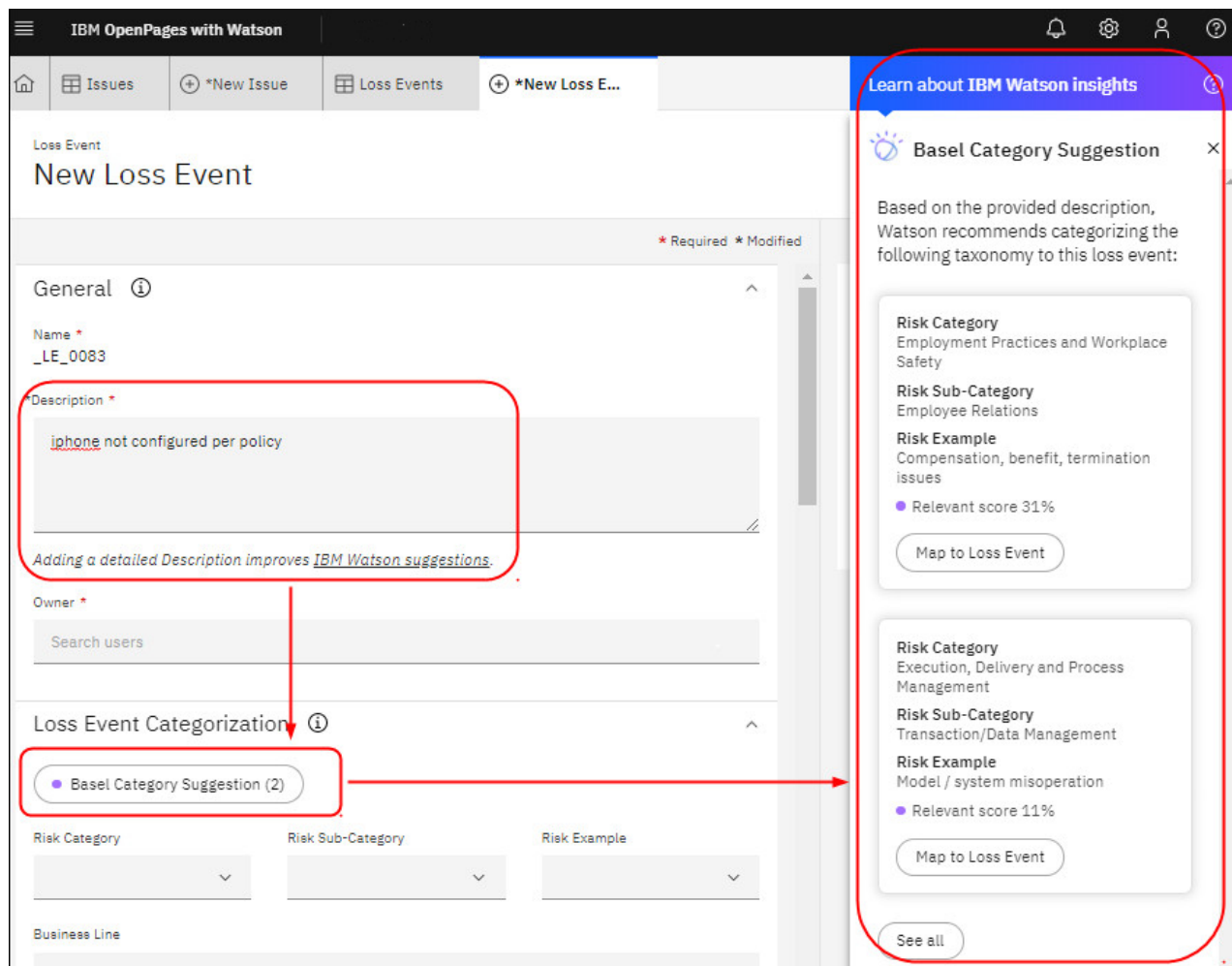


Figure 32. Example of a Classifier field that makes taxonomy suggestions

On the JSON tab, no properties are needed for taxonomy classifier fields.

Procedure

1. In the View Designer, click the **Design** tab.

The palette is displayed.

2. Drag the classifier input field either from the palette or the canvas and add it to a section or group.
3. Drag the classifier field either from the palette or the canvas and add it to a section or group. It is this field that is replaced with an IBM Watson Insights button.

Although it might make sense to place the two fields near each other, they can be in different groups or sections.

4. Click **Done**.

Adding a business entity selector field

A business entity selector field enables users to quickly identify the role a business entity plays.

Before you begin

The business entity selector field must already be configured in the Standard UI. For more information, see [“Configuring the Business Entity Selector display type for simple string fields \(Standard UI\)”](#) on page 350.

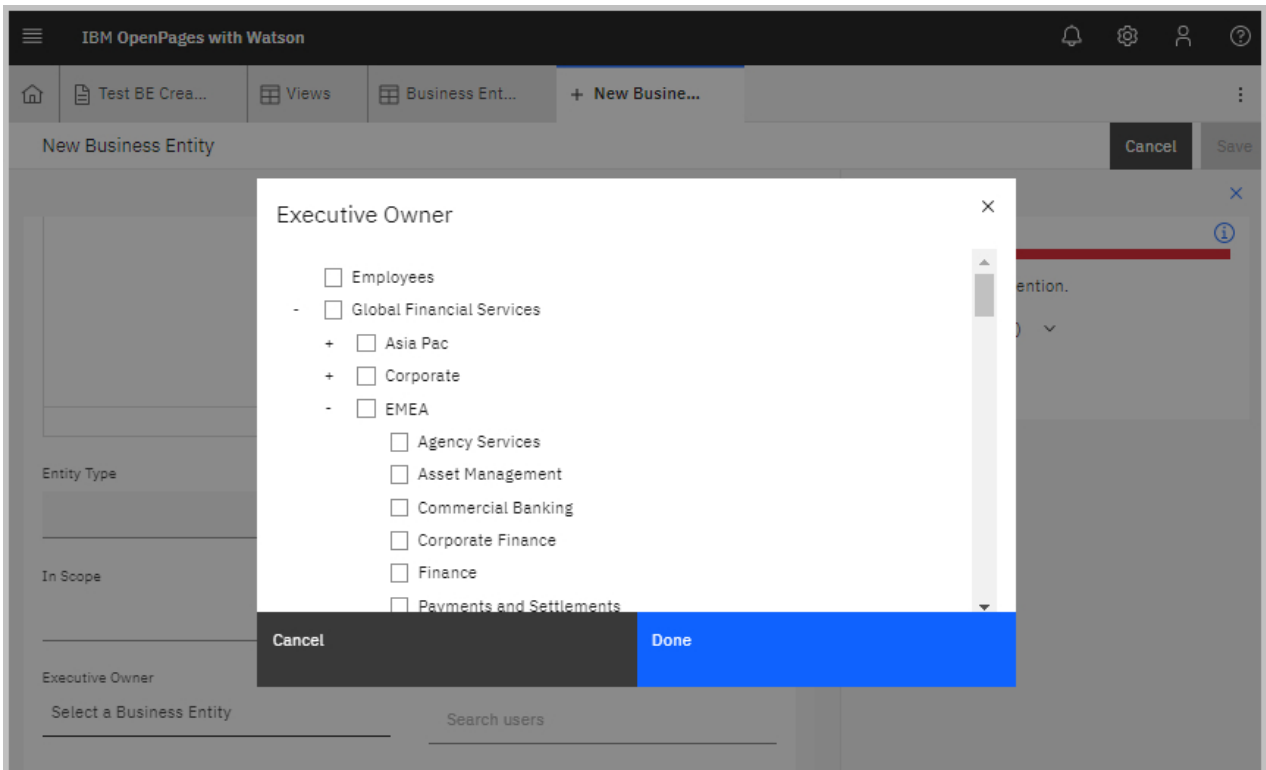
About this task

Business entity selector fields can be added to Grid Views, Creation Views, and Tasks Views.

Business entity selector fields can be added as key fields in user guidance.

In GRC Workflow, business entity selector fields can be used in task view override fields. They can also be used in conditions and validations. The options are Empty or Not empty.

The following example shows how a business entity selector field is rendered in a Creation View.



Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. On the canvas, drag a field that is defined as a business entity selector field to the canvas. The field attribute panel opens.
3. Set **Read Only** to true or false.
4. Set **Required** to true or false.
5. Add rules (optional). For more information, see [“Configuring rules” on page 439](#).
6. Click **Done**.
7. Publish the view.

Adding and configuring relationship fields on views

You can use relationship fields to support actions and render an object's associations to other objects in various graphical formats.

You can add the following types of relationship fields to views:

- Card
- Chart
- Count
- Grid
- Tree

You can apply rules to a relationship field, add actions to it, and control the related objects that are displayed within it.

Controlling whether a relationship field is visible, hidden, editable, read only, or required

You can apply **Rules** to all types of relationship fields. Rules allow you to more precisely control whether a relationship field is visible or hidden. For cards and grids, you can use rules to control some aspects of what users can do with related objects. For information, see [“Adding rules to relationship fields” on page 432](#).

Adding actions to a relationship field

You can add actions to cards and grids. You use an action, for example, to add, copy, or associate objects. For example, in a Task View for a Risk object, you might want to use an action that can associate a Control object to the object that is open in the view. For more information, see [“Adding actions to relationship fields” on page 434](#).

Controlling the objects that are displayed in a relationship field

The **Relationship Type** property controls the objects included in a relationship field based on the relationship between two object types: the object type for the view and the object type given in a relationship field.

The **Relationship Type** property exists on all types of relationship fields. Depending on the object type, it can be set to the following values:

- Children
- Parents
- Ancestors

- Descendants
- Siblings

The **Object Type** property controls the objects included in a relationship field based on the object type given in a relationship field. The **Object Type** property exists on all types of relationship fields except tree and all relationship types except siblings.

A sibling relationship type is to another object type that has the same parent. The allowed path is up to a parent object type and down to any other object type below that parent. For example, in a view for Controls, a relationship field can show other Controls that have the same parent Risk. A relationship field for a sibling relationship type has no **Object Type** property, instead it has **Parent Object Type** and **Sibling Object Type** properties. Sibling relationship type can be used in all relationship fields except trees. The sibling relationship type does not support actions.

You can apply the following filters to further restrict the objects that are included in a relationship field:

- You can apply a **Public Filter** to all types of relationship fields (card, chart, count, grid, or tree) and to any relationship type (Children, Parents, Ancestors, or Descendants). You use **Public Filter** to restrict the objects in a relationship field to those that meet the criteria of the specified public filter. If **Public Filter** is hidden in the property panel, no public filters for the object type exist.

For information about how to define a public filter for an object type, see [“Adding filters to object types \(Task Focused UI\)” on page 271](#). Even if the public filter is used only in the Task Focused UI, you must still associate it with a filtered list view in the Standard UI. For information, see [“Associating filters to Filtered List view and Grid view pages” on page 334](#).

- You can apply a **Relationship Path** to a card, chart, count, or grid. You use **Relationship Path** to restrict the objects in a relationship field if the relationship type is Ancestors or Descendants.

If you provide multiple filters, the filters are combined with an AND statement. An object must match all the filters to be included in the relationship field.

Organizing relationship fields in tab groups

Use tab groups to maximize the use of space and improve usability. For more information, see [“Organizing relationship fields in tab groups” on page 433](#).

Adding a card layout

Use a card layout to display text-based information about a series of objects and make viewing and comparing multiple objects easy. It can also be used to add parent and child objects and select objects to work on.

About this task

Card layouts are valid in Creation Views and Task Views.

A card layout shows related objects in boxes and supports actions. It is suited, for example, for displaying related regulations or parent business entities.

Use a card layout when only a few objects, for example, less than five, are expected to be displayed. Use a grid layout if you expect numerous objects to be displayed.

The **Fields** property controls the fields that are displayed in the relationship field. You can control what field the information is sorted by and the sort order.

If you choose an actor field in **Sort By**, the values are sorted by username (not first name and last name). The sort is case-sensitive.

In the following example, a loss event is open and each card shows a related mandate.

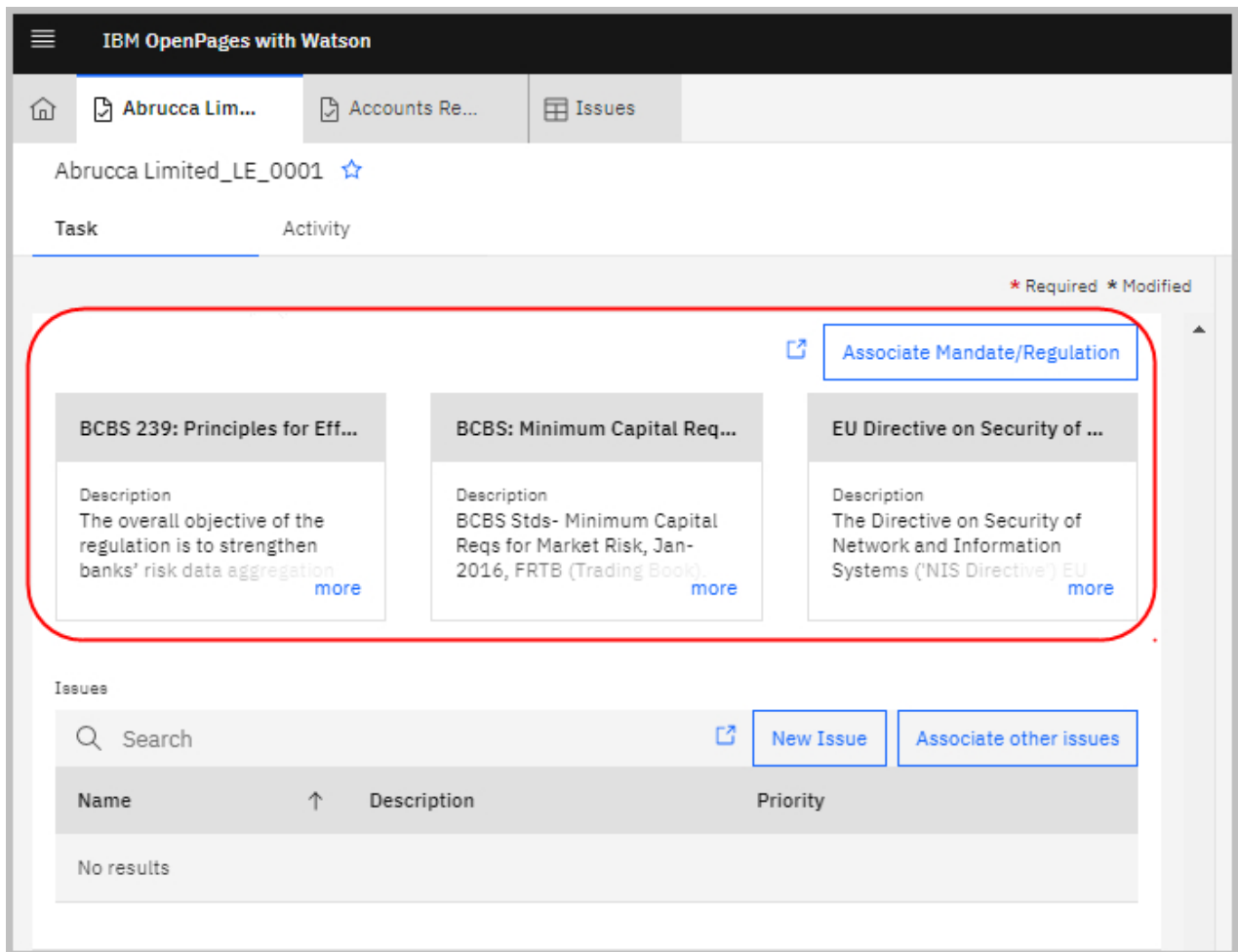


Figure 33. Example of a card layout

You can find an example in: SysView-Task-LossEvent.

On the JSON tab, a card layout is defined with *type* as relationship and *subDisplayType* as card.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a Card element from the palette and add it to a section.
3. Enter a **Label**. It displays as a field header within a section. Click **Edit** to enter localized values.

If it is displayed, click [Auto Translate](#)  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

4. Choose an option in **Relationship Type**:
 - Children
 - Parents
 - Descendants
 - Ancestors
 - Siblings
5. Choose an **Object Type** (displays for all relationship types except siblings). The objects that are listed vary depending on what you chose in **Relationship Type**.

6. Choose a **Parent Object Type** and a **Sibling Object Type** (displays only if **Relationship Type** is Siblings).
7. Complete the remaining fields. The fields that are listed vary depending on what you chose in **Relationship Type**.
8. Select a **Public Filter**, if one exists for the object type (optional).
9. Click **Add Action** to display an action button in the card (displays only if **Relationship Type** is Children or Parents).

If **Relationship Type** is Children, you can add the following types of actions:

- Add New
- Associate
- Copy Recursive
- Get Watson Suggestion

If **Relationship Type** is Parents, you can add the following types of actions:

- Associate Primary Parent
- Associate
- Get Watson Suggestion

For information about actions, see [“Adding actions to relationship fields” on page 434](#).

10. Choose a **Relationship Paths** (displays only if **Relationship Type** is Ancestors or Descendants).
11. Add **Fields** to the relationship field.
12. Choose a field in **Sort By**.
13. Define the **Sort Direction**.
14. Add rules to the relationship field (optional). For information, see [“Adding rules to relationship fields” on page 432](#).
15. Click **Done**.

What to do next

Place the card in a tab group (optional). For more information, see [“Organizing relationship fields in tab groups” on page 433](#).

Adding a chart diagram

Use a chart diagram when you want to view related objects in a graphic format based on a specific field.

About this task

Chart diagrams are valid in Task Views.

A chart is based on one object type and one field within that object type that is a single value enumerated field.

You can drill through the chart and open related objects.

The **Relationship Type** property controls the object relationships that are included in the chart diagram.

The following chart types are supported:

- Bar
- Doughnut
- Gantt
- Heat map (count-based and zone-based)
- Horizontal bar
- Pie

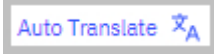
- Single stacked bar

For examples, see [“Chart diagram examples”](#) on page 418.

Note: Workflow fields are currently not supported in charts.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a Chart element from the palette and add it to a group or a section.
3. Enter a **Label**. It displays as a field header within a section. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator”](#) on page 1018.

4. Choose an option in **Relationship Type**:
 - Children
 - Parents
 - Descendants
 - Ancestors
 - Siblings
5. Choose an **Object Type** (displays for all relationship types except siblings). The objects that are listed vary depending on what you chose in **Relationship Type**.
6. Choose a **Parent Object Type** and a **Sibling Object Type** (displays only if **Relationship Type** is Siblings).
7. Choose an option in **Chart Type**:
 - Bar
 - Doughnut
 - Gantt
 - Heat Map
 - Horizontal Bar
 - Pie
 - Single Stacked Bar
8. If you choose Gantt, complete the Gantt Chart Configuration fields:
 - a) Select a **Start Date Field**.
 - b) Select an **End Date Field**.
 - c) Select a **Primary Row Field**.
 - d) Optional: Select a **Secondary Row Field**.
 - e) Select a **Color Definition Field**.
 - f) Click **Done**.

For more information about Gantt charts, see [“Chart diagram examples”](#) on page 418.

9. If you choose Heat Map, complete the following fields:
 - a) Select a field in **Horizontal Axis Field**.
 - b) Select a field in **Vertical Axis Field**.
 - c) Choose Count-based or Zone-based in **Color Assignment Type**.
 - d) Choose Categorical or Monochromatic in **Color Palette**.

The next field that is displayed is either **Color Ranges** or **Chart Colors**, depending on whether the heat map is count-based or zone-based.

- e) Assign colors to count ranges in **Color Ranges** (count-based only). For more information about color ranges, see [“Apply colors to value ranges”](#) on page 408.
 - f) The heat map is pre-displayed in **Chart Colors** (zone-based only). Assign a color to each cell.

Enumerated values that are defined as hidden are not displayed in **Chart Colors**. However, enumerated values that are hidden are displayed as gray when the heat map is rendered if the value has data.
 - g) Add rules (optional) and click **Done**. Disregard the steps below.
10. Select a **Public Filter**, if one exists for the object type (optional).
 11. Choose a **Relationship Paths** (displays only if **Relationship Type** is Ancestors or Descendants).
 12. Choose a field in **Chart Data Field** (displays for all types of charts except Gantt and heat map).
 13. In **Method Type** choose Count, Sum, Average, Min, or Max (displays for all types of charts except Gantt and heat map). If you chose Sum, Average, Min, or Max, provide a field in **Aggregation Field**. Only currency, decimal, and integer type fields are displayed in **Aggregation Field**.
For more information, see [“Examples: Bar charts”](#) on page 419.
 14. Choose Categorical or Monochromatic in **Color Palette** (displays for all types of charts except Gantt).
 15. In **Chart Colors**, apply colors to field values (displays for all types of charts except heat map).
For information, see [“Apply colors to enumerated field values”](#) on page 407.
 16. Add rules to the relationship field (optional). For information, see [“Adding rules to relationship fields”](#) on page 432.
 17. Click **Done**.

What to do next

Place the chart in a tab group (optional). For more information, see [“Organizing relationship fields in tab groups”](#) on page 433.

Chart diagram examples

Example: Doughnut chart

In the following example, a Business Entity is open and the doughnut chart shows its related risks by residual risk ratings. Click in the chart to drill down to the underlying objects.

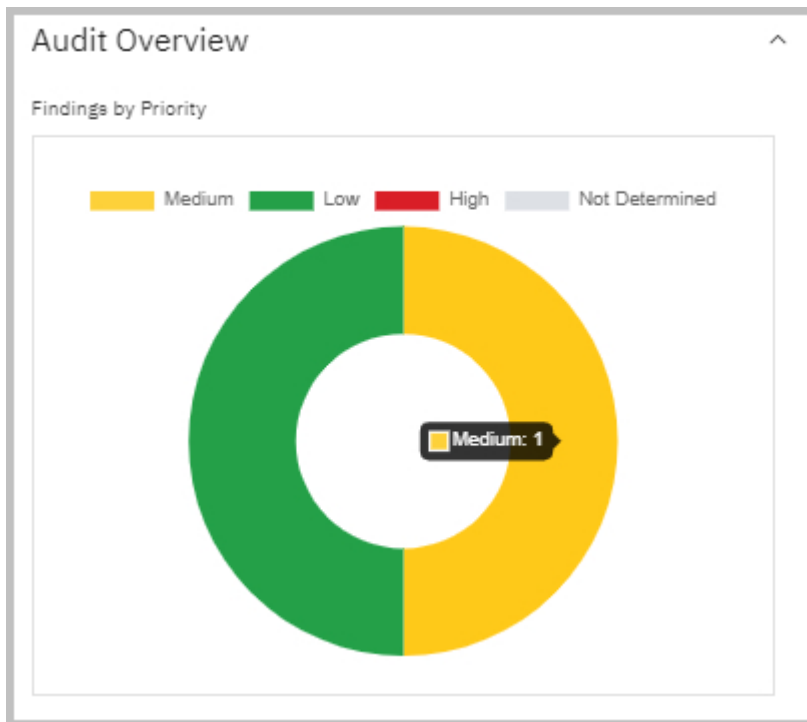


Figure 34. Example of a doughnut chart

Examples: Bar charts

In the following examples, a bar chart on the Dashboard is based on Loss Events. The **Chart Data Field** is set to Risk Category, which defines the colored bars in the chart.

In the following example, the **Method Type** is defined as Count. The results is that the chart shows the number of objects in each Risk Category.

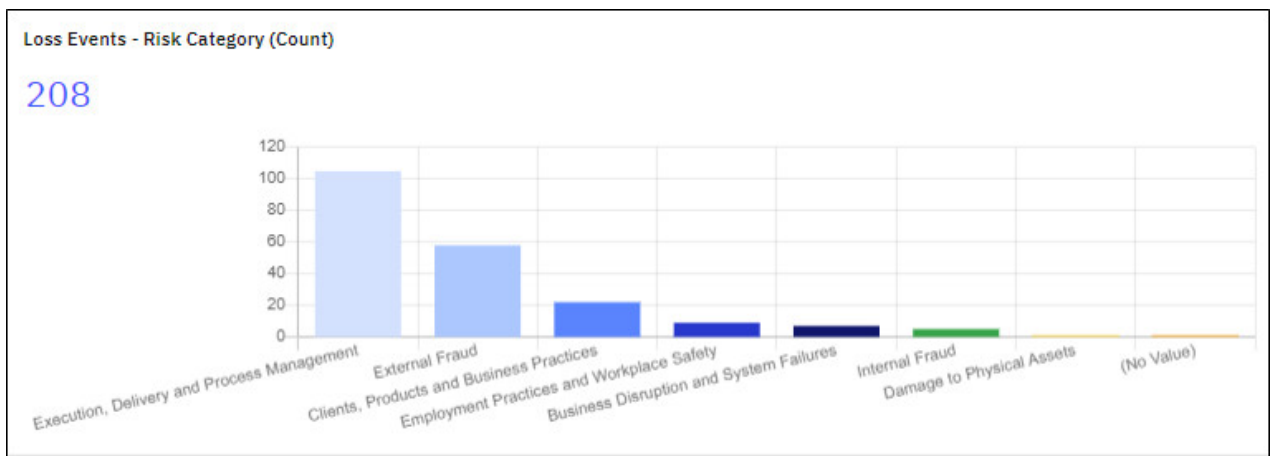


Figure 35. Bar chart with Method Type defined as Count

In the following example, the **Method Type** is defined as Max and the **Aggregation Field** is set to Gross Loss. The result is that the chart shows the maximum Gross Loss value for objects in each Risk Category.

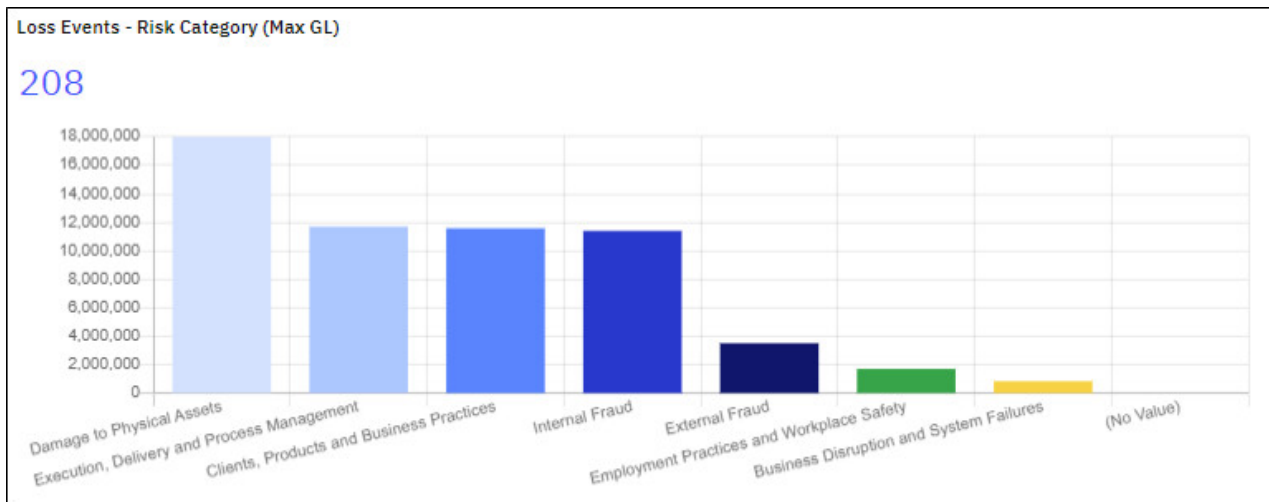


Figure 36. Bar chart with Method Type defined as Max and Aggregation Field set to Gross Loss

Example: Gantt chart

Use a Gantt chart when you want to view project or task assignment status over time. Gantt charts are typically used to view work assigned to a team or an individual person.

When you define a Gantt chart, you define the fields that make up the horizontal and vertical axes:

- The horizontal axis is a date range of two date fields that you choose. Note that system date fields cannot be used as date fields in Gantt charts.
- The vertical axis is one mandatory field and one optional field on the object type.

The order of the dates on the horizontal axis increases from left to right. The order of the fields on the vertical axis depends on the field definition. For string values, the order is alphabetical. For enumerated values, the order is the same as the order that is declared in the field definition if it is an enumerated value. The order of both axes is fixed and cannot be changed.

A Gantt chart can be opened from the following access points:

- A Task View
- A Dashboard panel that a user created
- A Dashboard panel that an administrator created

The access point determines how filtering is applied. If a Gantt chart is opened from:

- A Task View, a public filter can be defined in the Gantt chart.
- A Dashboard panel that a user created, either a public or private filter can be defined in the Dashboard panel.
- A Dashboard panel that an administrator created, a public filter can be defined in the Dashboard panel.

The access point determines what happens when you click a row in a Gantt chart. If a Gantt chart is opened from:

- A Task View, the object opens in a Quick View.
- A Dashboard, the object opens in a Task View in a new tab.

Coloring in a Gantt chart depends on colors assigned to the primary and secondary fields. If no colors are assigned to the field values in a view, the rows display as gray. If the field values are assigned a color in a view, those colors are applied. To override the colors or if neither field is an enumerated field, you must define colors in **Color Definition Field**.

Gantt charts become less useful when they contain a lot of data. For this reason, apply filters and keep the date range short. Up to 425 items can be displayed vertically.

For example, a useful Gantt chart is one that shows Plans that are associated with an Audit. The horizontal axis can show the date range of Expected Start Date to Expected End Date. The vertical axis can list the auditors and activities.

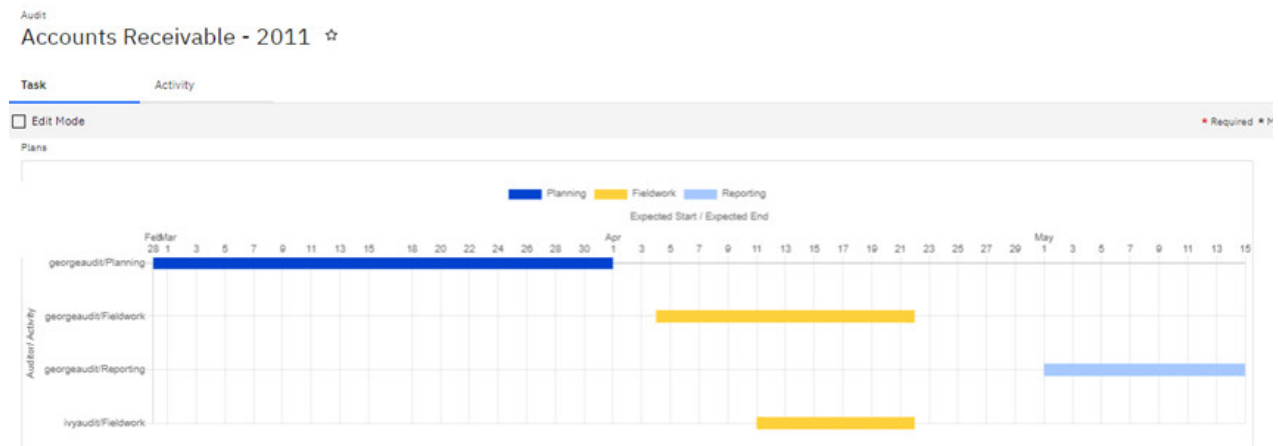


Figure 37. Gantt chart

Example: Heat map (count-based)

Use a count-based heat map when you want to see a data distribution chart, where colors are assigned to counts rather than zones in the chart. You use the colors to apply emphasis to the counts in the chart.

When you define a count-based heat map, you define the two fields that make up the horizontal and vertical axes and the colors for the enumerated value ranges.

The order of the values on the horizontal axis is the same as the order that is declared in the field definition. The same is true for the vertical axis but the order is reversed. The order can be changed in the field definition, but the order of the items in all drop downs is affected.

In the following example, a Business Entity is open and a count-based heat map chart shows its related loss events. Each cell contains a count of objects at value intersect points for Risk Category and Business Line. There are, for example, 32 loss events categorized as External Fraud and Asset Management. A user can click in a cell to drill down to the underlying objects.

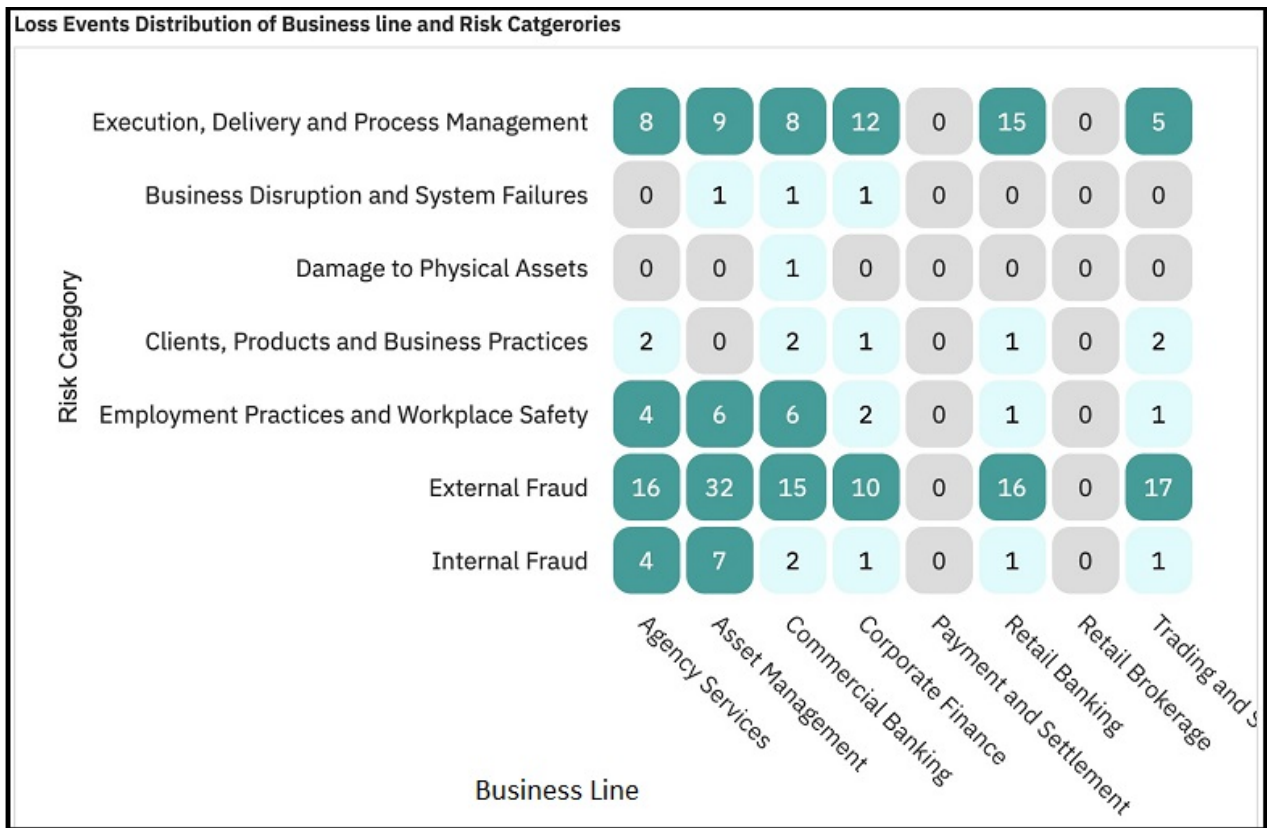


Figure 38. Count-based heat map based on Risk Category (vertical axis) and Business Line (horizontal axis)

Example: Heat map (zone-based)

Use a count-based heat map when you want to see a data distribution chart, where colors are assigned to cells in the chart rather than counts. You use the colors to apply emphasis to the value intersects in the chart.

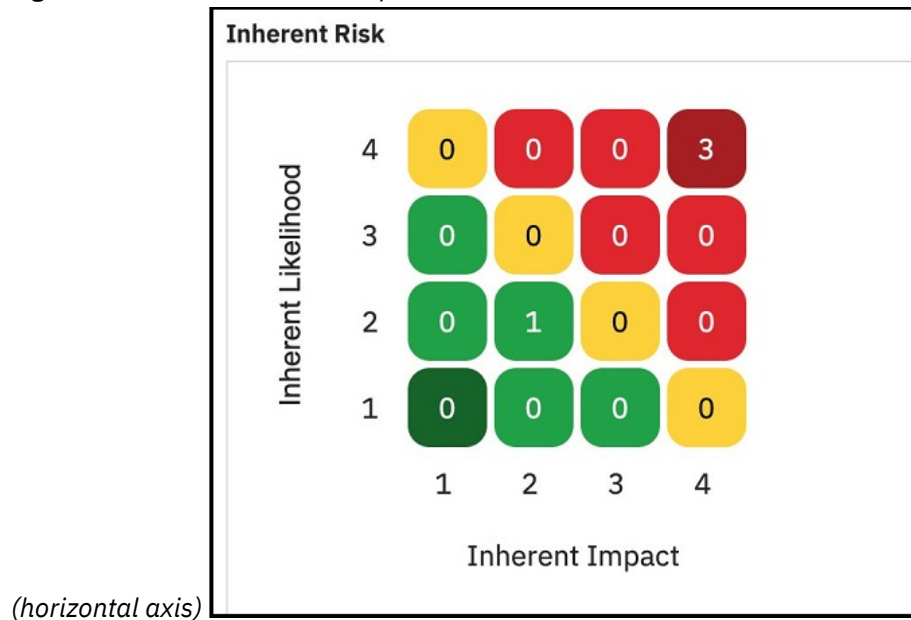
When you define a zone-based heat map, you define the two fields that make up the horizontal and vertical axes, and assign colors to cells (zones) in the map.

The order of the values on the horizontal axis is the same as the order that is declared in the field definition. The same is true for the vertical axis but the order is reversed. The order can be changed in the field definition, but the order of the items in all drop downs is affected.

In the following example, a Risk Assessment is open and a zone-based heat map chart shows its related risks organized by inherent risk. Each cell contains a count of objects that have value intersects for Inherent Likelihood and Inherent Impact. There are, for example, 3 risks whose Inherent Likelihood and Inherent Impact are both 4. Regardless of the count, the value intersect where Inherent Likelihood and Inherent Impact are both 4 is always red and in the upper right corner.

A user can click in a cell to drill down to the underlying objects.

Figure 39. Zone-based heat map based on Inherent Likelihood (vertical axis) and Inherent Impact



Example: Horizontal bar

In the following example, an Audit is open and a horizontal bar chart shows its related work papers by review status. Click in the chart to drill down.

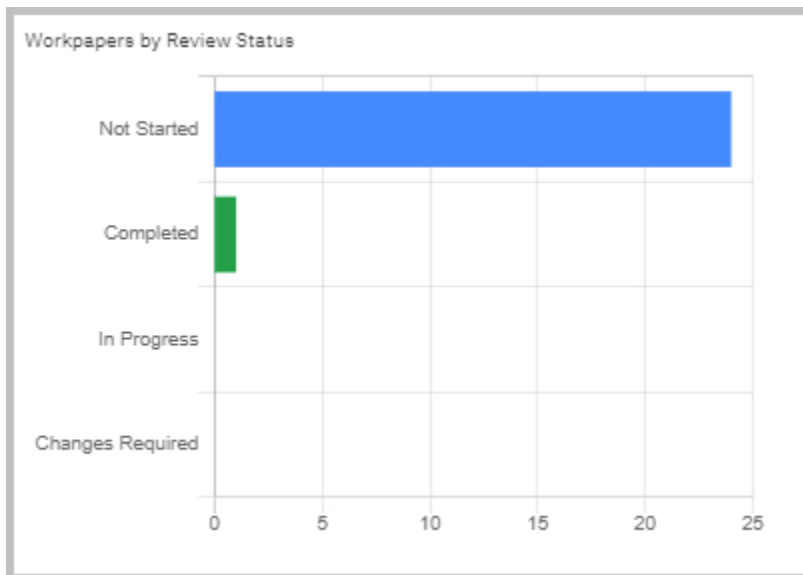


Figure 40. Example of a horizontal bar chart

Example: Single stack bar

In the following example, an Audit is open and a single stack bar chart shows its related work papers by review status. You can quickly understand that most of the work papers for this audit have not yet been started.

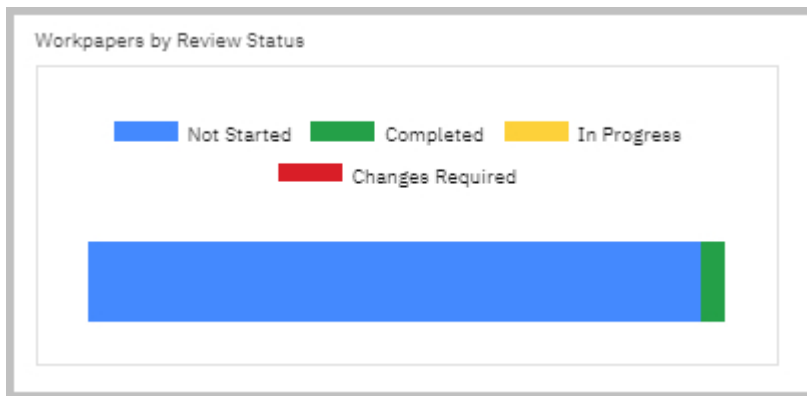


Figure 41. Example of a single stack bar chart

Click in the different areas of a chart to open a Grid View that lists the underlying objects for that value. For example, click in the teal area and a Grid View opens that lists work papers that are related to this audit and whose review status is "Not Started". Click in the green area and a Grid View opens that lists work papers that are related to this audit and whose review status is "Completed".

Indicators at the top of the Grid View show the filters that are applied and the number of objects in the list. Click the arrow icon to open a parent object. Click the X to remove a filter and update the list in the Grid View.

Name	Description	Preparer	Reviewer	Type
02-01-WP01 Internal Audit > FinAud > FinAud 1 > Accounts Receivable - 2011	Comparative Summary	georgeaudit	kevinaudit	Test Evid
02-01-WP02 Internal Audit > FinAud > FinAud 1 > Accounts Receivable - 2011	Detailed List of Accounts Receivable	georgeaudit	kevinaudit	Test Evid
02-01-WP03 Internal Audit > FinAud > FinAud 1 > Accounts Receivable - 2011	Evaluate Reconciling Items	georgeaudit	kevinaudit	Test Evid
02-01-WP04 Internal Audit > FinAud > FinAud 1 > Accounts Receivable - 2011	Investigate Significant Unusual Items	georgeaudit	kevinaudit	Test Evid

Figure 42. Grid View of underlying objects in a chart

Adding a count

Use a count to provide quick access to items that need to be worked on. Valid in Task Views.

About this task

Counts are valid in Task Views.

A count shows an object count. Click the count to open a Grid View that lists parent or child objects.

The **Relationship Type** property controls the object relationships that are included in the count diagram.

The **Object Type** property controls the object type that is counted.

Color palettes cannot be applied to counts.

In the following example, a risk assessment is open and the count is for SOXControl objects. You can see how many objects exist and drill down into the count.



On the JSON tab, a count is defined with *type* as relationship and *subDisplayType* as count.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a Count element from the palette and add it to a group or a section.
3. Enter a **Label**. It displays as a field header within a section. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

4. Choose an option in **Relationship Type**:
 - Children
 - Parents
 - Descendants
 - Ancestors
 - Siblings
5. Choose an **Object Type** (displays for all relationship types except siblings). The objects that are listed vary depending on what you chose in **Relationship Type**.
6. Choose a **Parent Object Type** and a **Sibling Object Type** (displays only if **Relationship Type** is Siblings).
7. Select a **Public Filter**, if one exists for the object type (optional).
8. Choose a **Relationship Paths** (displays only if **Relationship Type** is Ancestors or Descendants).
9. Define **Color Ranges**.

For information, see [“Apply colors to value ranges” on page 408](#).

10. Add rules to the relationship field (optional). For information, see [“Adding rules to relationship fields” on page 432](#).
11. Click **Done**.

Adding a grid layout

Use a grid layout to add parent and child objects, compare objects, upload files (attachments), and select objects to work on.

About this task

Grid layouts are valid in Creation Views and Task Views.

A grid shows related objects in a table and supports actions. It is well suited, for example, for uploading files and adding parent or child objects.

From a Task View, objects that are listed in a grid are initially sorted alphabetically by object name. The user can then change the sorting. From a Creation View, objects that are listed in a grid are not initially sorted, and the user cannot change the sorting.

From a Task View, if you click a row in the grid, the object opens in a Task View in a new tab.

From a Task View, if you click  next to an object in the grid, the object opens in a Quick View. A Quick View is a Task View that is displayed in a small sidebar. A Quick View has all the functionality of a Task View with a few exceptions. Quick View is always available in a grid layout and requires no configuration.

From a Task View, if you click the field label of the relationship field, a Grid View with the same filter criteria opens. You can move between this Grid View and the Task View where you started.

A search box is always displayed in a Task View. A search box is not displayed in a Creation View.

Consider performance when you design Grid relationship fields for object types that potentially display a large number of objects. For quicker system performance, apply a public filter to a relationship field. On actions, apply folder filters and filter rules.

The **Fields** property controls the fields that are displayed in the relationship field. You can control what field the information is sorted by and the sort order.

To use the relationship field to upload files in task views, choose File in **Object Type**. The **Fields** property includes only **File Name** by default. You can optionally add other fields to display in the relationship field. If **Description** is not included in the **Fields** property, a user can still add a description when they select a file to upload.

Note: If you edit the JSON and make **Description** read-only, a user cannot add a description when they select a file to upload. If you make **Description** required and read-only, a user cannot upload a file.

Additionally, you must define a task view for files (SOXDocument). For information, see [“Defining Task Views for file object types”](#) on page 395. It is not possible to upload files in a creation view.

If you choose an actor field in **Sort By**, the values are sorted by username (not first name and last name). The sort is case-sensitive.

In the following example, a business entity object is open and you can add a parent business entity.

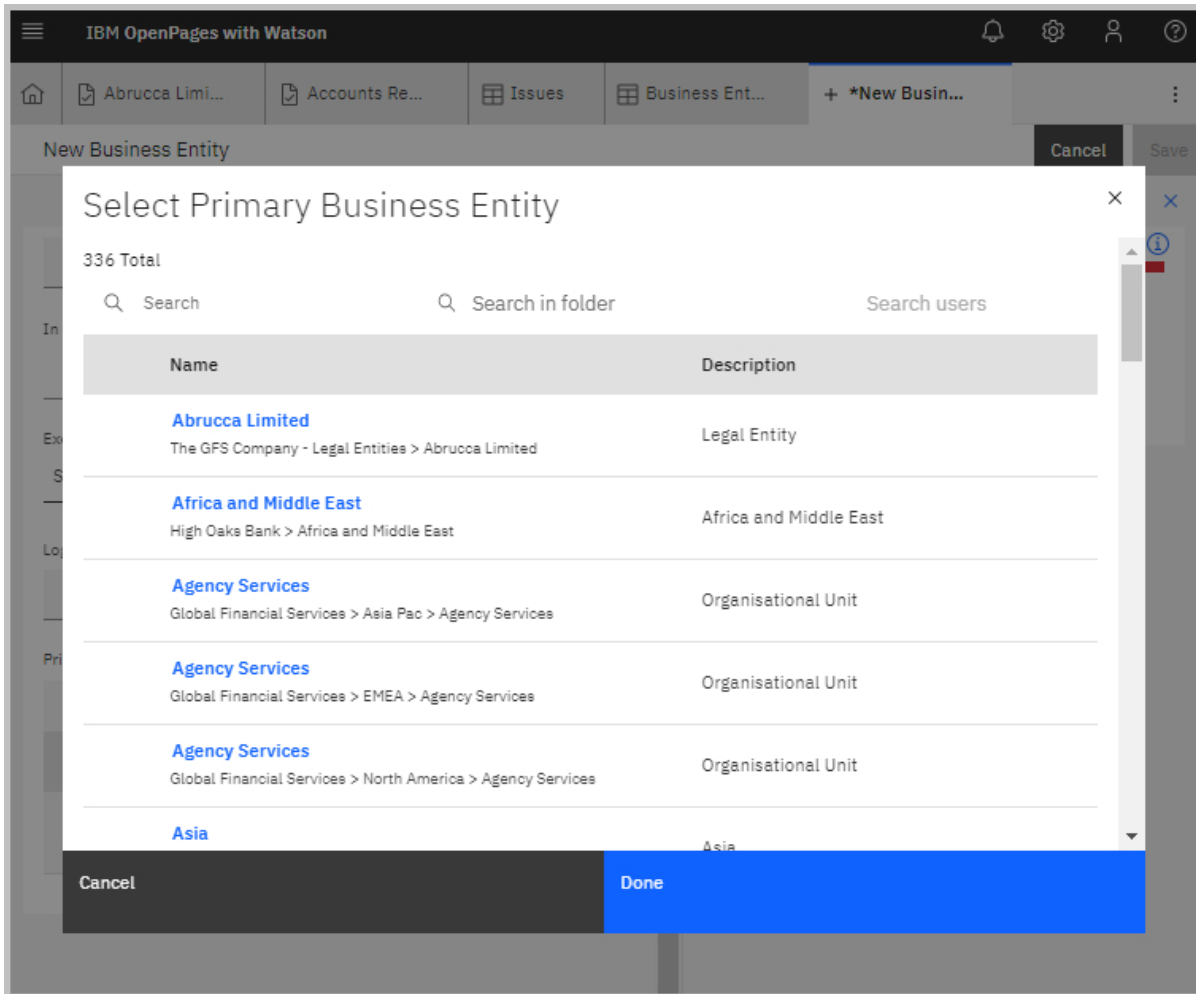


Figure 43. Example 1: Adding a primary parent

In the following example, a task view contains a grid relationship field for files. An Audit object is open and you can upload a file by clicking **Add/Update** or dragging and dropping a file to the task view.

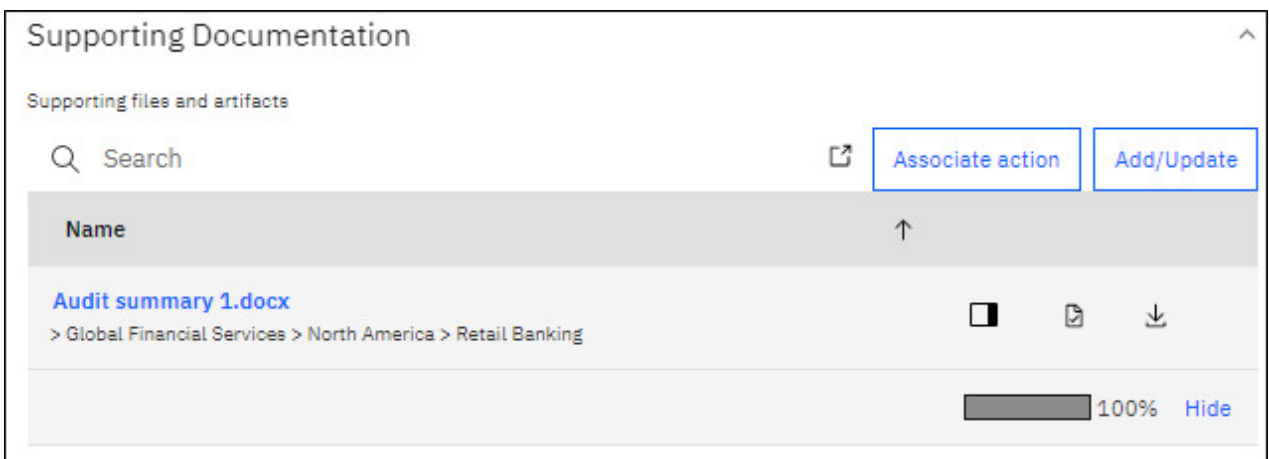
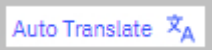


Figure 44. Example 2: uploading files

You can find grid view examples in SysView-Task-SOXBusEntity and SysView-Task-SOXControl. On the JSON tab, a grid layout is defined with *type* as relationship and *subDisplayType* as grid.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a Grid element from the palette and add it to a section.
3. Enter a **Label**. It displays as a field header within a section. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

4. Choose an option in **Relationship Type**:
 - Children
 - Parents
 - Descendants
 - Ancestors
 - Siblings
5. Choose an **Object Type** (displays for all relationship types except siblings). The objects that are listed vary depending on what you chose in **Relationship Type**.
6. Choose a **Parent Object Type** and a **Sibling Object Type** (displays only if **Relationship Type** is Siblings).
7. Select a **Public Filter**, if one exists for the object type (optional).
8. Click **Add Action** to display an action button in the card (displays only if **Relationship Type** is Children or Parents).

If **Relationship Type** is Children, you can add the following types of actions:

- Add New
- Associate
- Copy Recursive
- Delete
- Get Watson Suggestion

If **Relationship Type** is Parents, you can add the following types of actions:

- Associate Primary Parent
- Associate
- Delete
- Get Watson Suggestion

For information about actions, see [“Adding actions to relationship fields” on page 434](#).

9. Choose a **Relationship Paths** (displays only if **Relationship Type** is Ancestors or Descendants).
10. Set **Required** to true to make it mandatory for a user to provide at least one object in the grid.
11. Choose a field in **Sort By**.
12. Define the **Sort Direction**.
13. Add rules to the relationship field (optional). For information, see [“Adding rules to relationship fields” on page 432](#).
14. Click **Done**.

What to do next

Place the grid in a tab group (optional). For more information, see [“Organizing relationship fields in tab groups” on page 433](#).

Adding a tree diagram

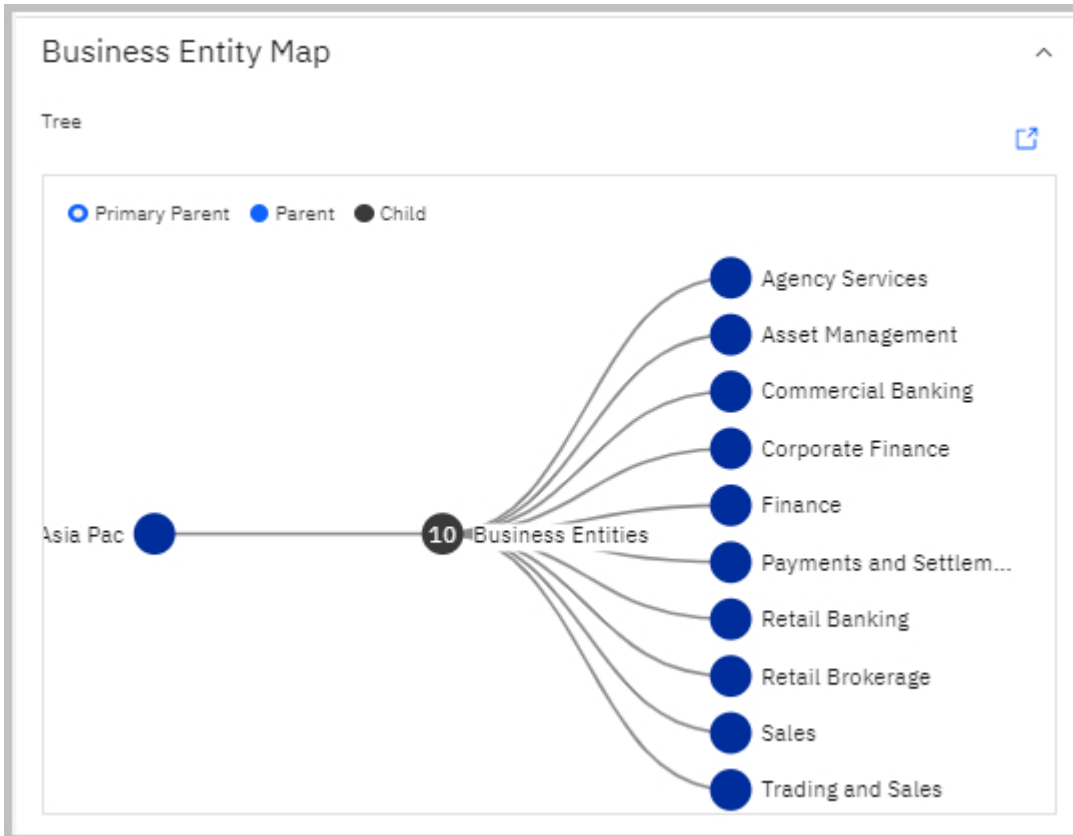
Use a tree diagram to display an object relationship diagram that allows users to interactively explore data and data relationships.

About this task

Tree diagrams are valid in Task Views.

A tree diagram displays an object relationship structure. You can see how an object is related to all other objects, parent objects, or child objects. You can also drill through the diagram and open objects.

In the following example, a business entity is open and all parent and child objects are displayed in a tree diagram.



You can find an example in: SysView-Task-SOXBusEntity.

On the JSON tab, a tree diagram is defined with *type* as relationship and *subDisplayType* as tree.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a Tree element from the palette and add it to a section.
3. Choose an option in **Relationship Type**:
 - blank (includes both Children and Parents)
 - Children
 - Parents
4. Add rules to the relationship field (optional). For information, see [“Adding rules to relationship fields”](#) on page 432.

5. Click **Done**.

What to do next

Place the card in a tab group (optional). For more information, see [“Organizing relationship fields in tab groups”](#) on page 433.

Adding a classifier field that makes object association suggestions

You can add classifier fields that make object association suggestions using a natural language processing service.

Before you begin

The natural language processing service must already be configured to make object association suggestions. For information, see [“Natural language processing services ”](#) on page 1021.

About this task

Classifier fields that make object association suggestions are valid in Creation Views and Task Views.

The Task Focused UI supports making taxonomy suggestions and object association suggestions. For information about taxonomy suggestions, see [“Adding a classifier field that makes taxonomy suggestions ”](#) on page 410 .

You can add multiple classifier fields to a view.

The classifier field and the classifier input field must both be in the view. The classifier target fields can optionally be included in the view. It is not necessary to configure the Watson statement on the classifier input field (*Adding a description improves IBM Watson Suggestions*), the IBM Watson Insights button, or the IBM Watson Insights panel. These elements display automatically for classifier fields.

The action label is the button label for the IBM Watson Insights button. The title of the IBM Watson Insights panel is the object type plus *Mapping*.

In this example, the text in the Description on a new Issue is used as input to a natural language processing service that can suggest appropriate Controls. The field that associates Controls is configured to be a classifier field.

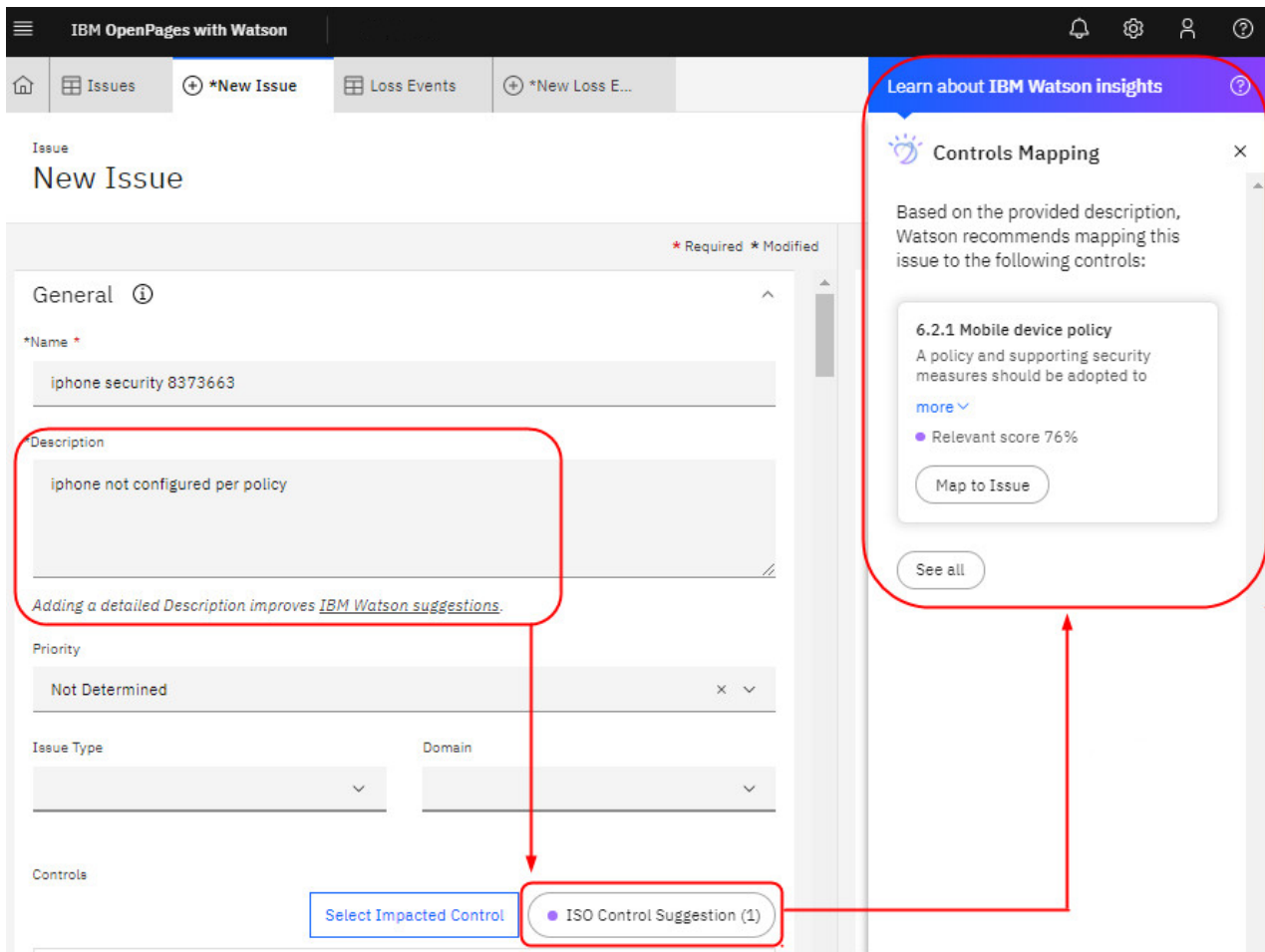


Figure 45. Example of a Classifier field that makes taxonomy suggestions

On the JSON tab, a classifier field is part of a card or grid relationship field and its *actionType* is set to *suggestAssociations*.

Procedure

1. Drag the classifier input field either from the palette or the canvas and add it to a section or group.
2. Drag the classifier field either from the palette or the canvas and add it to a section or group.
3. Create a card or grid relationship field and follow all steps until you define an action. For information, see [“Adding a card layout” on page 414](#) or [“Adding a grid layout” on page 425](#).
4. Click **Add Action** and choose **Watson Suggestion**.
 - a) Enter a **Label**. It displays as a button label. Click **Edit** to enter localized values.

If it is displayed, click [Auto Translate](#)  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

- b) Select the classifier field you already put on the canvas in **Classifier Field**. The system lists only classifier fields that are on the canvas.

Although it is not required, it might make sense to place the classifier field near the card or grid relationship field that uses it.

- c) Click **Done**.

5. Finish defining the relationship field.

Adding rules to relationship fields

You can apply **Rules** to all types of relationship fields (cards, charts, counts, grids, and trees).

About this task

Rules allow you to more precisely control whether a relationship field is visible or hidden. For cards and grids, rules can also control some aspects of what users can do with related objects.

Rules on relationship fields are based on the fields for the object type of the view. For example, if you are building a view for Risk objects and the relationship field is for Control objects, the rules are based on fields for the Risk object not the Control object.

In a rule, you specify a condition that checks for the existence of any value of a field or specific values of one or more fields on a object. If the condition is met, the rule is applied to the relationship field.

In all types of relationship fields (cards, charts, counts, grids, and trees), you can apply the following rule types:

- **Visible**

Shows the relationship field in a view if the rule is met.

- **Hidden**

Hides the relationship field in a view if the rule is met.

In cards and grids, you can apply the following additional rule types:

- **Editable**

Makes buttons in a card or grid visible and actionable if the rule is met.

- **Read Only**

Hides buttons in a card or grid if the rule is met. Users can view objects in the card or grid but cannot change them.

- **Required**

Makes it mandatory for the user to provide one object in a card or grid if the rule is met.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. First, move the fields that are used in the rule from the palette to the canvas.
In the following steps, the options in **Rule Type** vary depending on the relationship field type.
3. In the property panel of a relationship fields, click **Add Rule**.
4. Select a **Rule Type**.
5. In **Controlled By**, choose **One field with any value** or **Multiple controllers or values**.
6. If you choose **One field with any value**:
 - a) Select a **Controlling Field**. The system lists fields for the object type of the view that are on the canvas.
 - b) Click **Done**.
7. If you choose **Multiple controllers or values**:
 - a) In **Controlling Field Logic** select **All controlling field conditions must be met** or **Any controlling field condition may be met**.
 - b) Click **Add Controller Field**.
 - c) Choose a field in **Controlling Field**. The system lists fields for the object type of the view that are on the canvas. The next selections depend on the field type.

- For actor fields, you can set **Match Current User** and/or select other users or user groups in **Other Users or Groups**. Any match on either field resolves the controller to true. If **Match Current User** is set to true, the signed on user must be the user or be in a user group for the value in the **Controlling Field**.
 - For enumerated type fields, click **Values** and you can choose one or more individual values.
 - Click **Done**.
- d) Add **Add Controller Field** to add the next controller field. Repeat the previous steps. Continue until all controller fields have been added. Although you can change the order of the controller fields, it has no effect in the view.
8. Click **Done**.

Organizing relationship fields in tab groups

You can organize the following types of relationship fields in tab groups: cards, charts, grids, and trees. Counts cannot be placed in tab groups.

About this task

Use tab groups to maximize the use of space and improve usability. Without tabs, relationship fields are listed vertically down the page and users must scroll down to view them.

A tab group can have up to six relationship fields. Each relationship field displays as a tab. The name of the relationship field is the tab label.

Tab groups can be added to Creation Views and Task Views. A Creation View or Task View can have multiple tab groups.

In the following example, a Risk object is open and six relationship fields are displayed in a tab group named, Tab Group Section. The first tab, Mitigating Controls, is open, and it is a grid relationship field.

The screenshot shows the IBM OpenPages with Watson interface. The top navigation bar includes 'Views', 'Control Task', 'Controls', 'CTL-02-04-0...', 'Risks', and 'RB-01-Risk...'. The main content area displays the 'Task' tab for 'RB-01-Risk00189'. Below the task details, there is a 'Tab Group Section' with six tabs: 'Mitigating Controls', 'Issue from Risk a...', 'Controls by Desig...', 'Controls by Opera...', 'KRI from Risk and...', and 'Tree'. The 'Mitigating Controls' tab is selected and active, showing a grid of controls. The grid has columns for 'Name', 'Control Owner', 'Design Effectiveness', and 'Operating Effectiveness'. The data rows show three controls, all with 'Effective' design effectiveness and 'Not Determined' operating effectiveness.

Name	Control Owner	Design Effectiveness	Operating Effectiveness
CTL-04-03-03-01 Global Financial Services > North America > Retail Banking	lcm	Effective	Not Determined
CTL-04-03-03-02 Global Financial Services > North America > Retail Banking	orm	Effective	Not Determined
CTL-04-03-03-03 Global Financial Services > North America > Retail Banking	iam	Not Determined	Not Determined

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a Tab Group from the palette to the canvas and place it in a section.
3. Enter a **Name**.
4. Click **Done**.
5. Add relationship fields to the tab group. Either create a new relationship field or drag an existing one from the canvas to the tab group.
6. Move the relationship fields up and down to control the order from left to right that they are displayed in the tab group.

Adding actions to relationship fields

You can use actions on relationship fields to add, copy, or associate objects.

You can add one or multiple actions to card and grid relationship fields.

Adding an Associate action

Define an action as **Associate** to associate parent or child objects. A Grid View opens where you can select or deselect objects.

About this task

Use an **Associate** action, for example, on a Task View for loss events if you want to add the ability to associate mandates.

A grid relationship field that is defined with an **Associate** action displays a **Remove** button when one or more already associated objects are selected. The **Remove** button allows you to disassociate objects (it does not delete objects). If the grid relationship field is required, all associated objects can be removed except for one. The **Remove** button displays automatically when an **Associate** action is configured for a grid relationship field. The **Remove** button does not display in card relationship fields.

To delete objects, use the **Delete** action. For information about providing the ability to delete objects, see [“Adding a Delete action” on page 438](#).

To associate a primary parent object, use the **Associate Primary Parent** action rather than **Associate**. For information, see [“Adding an Associate Primary Parent action” on page 435](#).

You can find an example in: SysView-Task-LossEvent.

On the JSON tab, an associate action is defined when *actionType* is set to associate in a card or grid relationship field.

Procedure

1. In a card or grid relationship field, click **Add Action** and choose **Associate**.
2. Enter a **Label**. It displays as a button label. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

3. Set **Multi Select** to true or false.
4. Click **Folder Filter** to restrict the objects that are available for selection in the Grid View to a specific folder.
5. Click **Filter Rules** to restrict the objects that are available for selection in the Grid View using a dynamic filter. For information see, [“Defining dynamic filters on actions in relationship fields” on page 438](#).

6. Click **Done**.

Results

If both **Folder Filter** and **Filter Rules** are provided, the filters are combined with an AND statement. An object must match both filters to be available for selection.

Adding an Associate Primary Parent action

Define an action as **Associate Primary Parent** to associate a parent object. A Grid View opens where you can select or deselect a single object. If the object does not have a primary parent, the one you choose is set to the primary parent. If the object has a primary parent, the one you choose overrides it.

About this task

For most object types, a Creation View must have a relationship field with an **Associate Primary Parent** action.

Use an **Associate Primary Parent** action, for example, on a Task View for loss events if you want to add the ability to add a primary parent and other business entities.

An **Associate Primary Parent** action does not display a **Remove** button when one or more already associated objects are selected. To display a **Remove** button, add an **Associate** action to the relationship field. The primary parent itself cannot be removed, but other objects can be. For more information, see [“Adding an Associate action” on page 434](#).

You can find an example in: SysView-Task-LossEvent.

On the JSON tab, an associate primary parent action is defined when *actionType* is set to *associatePrimary* in a card or grid relationship field.

Procedure

1. In a card or grid relationship field, click **Add Action** and choose **Associate Primary Parent**.
2. Enter a **Label**. It displays as a button label. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

3. Click **Folder Filter** to restrict the objects that are available for selection in the Grid View to a specific folder.
4. Click **Filter Rules** to restrict the objects that are available for selection in the Grid View using a dynamic filter. For information see, [“Defining dynamic filters on actions in relationship fields” on page 438](#).
5. Click **Done**.

Results

If both **Folder Filter** and **Filter Rules** are provided, the filters are combined with an AND statement. An object must match both filters to be available for selection.

Adding an Add New action

Define an action as **Add New** to create a new object. The Creation View for the object type opens. The Add New action is available only if **Relationship Type** is Children.

About this task

You can find an example in: SysView-Task-LossEvent.

On the JSON tab, an add new action is defined when *actionType* is set to addNew in a card or grid relationship field.

Procedure

1. In a grid or card relationship field, click **Add Action** and choose **Add New**.
2. Enter a **Label**. It displays as a button label. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

3. In **Add New Behavior**, choose **Tab** or **Sidebar** to define where the Creation View opens. **Tab** opens the Creation View in a new tab. **Sidebar** opens the Creation View in a Quick View side panel of the Task View that is already open.

If you select **Sidebar**, the Creation View can only create new child objects for the parent object that is open. No other associations are supported in the sidebar. Verify that the Creation View does not contain any other association actions.

4. Click **Done**.

Adding a Copy Recursive action

Define an action as **Copy Recursive** to copy an existing object and associate it to an object that is open in a Task View. The action can be defined to make copies of objects that are associated to a source object and to copy parent associations from a source object to a new object.

About this task

The **Copy Recursive** action can be used in cards and grids in Task Views. The **Relationship Type** must be Children.

A **Copy Recursive** action can be used, for example, in a Task View for Process objects to allow users to make copies of existing Risk and Control objects. When a user accesses the Task View, a grid relationship field displays Risk objects that are already associated with the open Process object and that match a **Public Filter**, if one is defined. When a user clicks a button for the copy action, Risks that meet the **Folder Filter** and **Filter Rules** criteria are listed. The list includes Risks that are already associated with the Process and those that are not. When a user selects a Risk and clicks Done, a copy of the selected source Risk object is created and associated to the Process that is open in the view.

Additionally, depending on how the **Copy Recursive** action is defined, copies are also made of the source object's child and grandchild objects, for a specified object type relationship. Only child objects that have the source object as their primary parent are copied. For example, when a Risk object is copied, copies of all child Control objects that have the Risk as their primary parent can also be made.

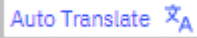
Additionally, depending on how the **Copy Recursive** action is defined, parent associations for a source object can be replicated to newly copied objects. For example, a newly copied Control can be associated to the same parent Requirement objects as the source Control object.

Depending on how workflows are configured, workflows can be started for the newly created objects and child objects. Workflows cannot be started on newly created grandchild objects.

On the JSON tab, a copy recursive action is defined when *actionType* is defined as copyRecursive in a card or grid relationship field.

Procedure

1. In a card or grid relationship field, click **Add Action** and choose **Copy Recursive**.
2. Enter a **Label**. It displays as a button label. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

3. Click **Folder Filter** to restrict the objects that are available for selection in the Grid View to a specific folder.
4. Click **Filter Rules** to restrict the objects that are available for selection in the Grid View using a dynamic filter. For information see, [“Defining dynamic filters on actions in relationship fields” on page 438](#).
5. Set **Auto Name Children** to true or false. If set to true, auto naming is applied to all newly copied objects (including children and grandchildren) in the object type relationship, given that auto naming is defined for the object type. For information about configuring auto naming, see [“Object auto-naming settings” on page 609](#).
6. For object types that are not configured to use auto naming, the **Conflict Behavior** setting determines what happens when a copied object has the same name as an existing object in a target location. Options are:
 - **overwrite** - a new version of the object in the target directory is created with all of the information of the copied object. All prior versions of the object in the target directory are maintained.
 - **copyof** - during the copy operation, any objects with the same name as an existing object in the target location will be renamed to "Copy of <objectname>".

Note: Consider carefully whether to use **overwrite** or **copyof** when you copy objects that have the same name coming from different hierarchies. The end result if you use **overwrite** will be a single object with many versions. However, if you use **copyof**, it will be many objects with one version.

 - **existing** - if a copied object has the same name as an object in the target location, that file will not be copied. All other objects (without duplicate names) will still be copied to the target location. If you choose this option, you should examine the results of copy operations to determine whether any associations between objects have changed as a result of the copy. For example, if an associated risk is not copied to the new location because an existing risk has the same name, the copied parent process of the risk will be associated with the pre-existing risk in the target location.
 - **Exception** - a message is displayed and the copy action is not completed.
7. Click **Set** in **Object Type**. The object type relationship structure from the source object type through its child and grandchild object types is displayed. Select each object type that is included in the recursive copy action.
8. Click **Add Associations** to define whether parent associations of source objects are replicated to newly copied objects.
 - a) Choose a **Child Type**. You can choose the object type for the relationship field or any of the objects types you selected in **Object Type**.
 - b) Choose a **Parent Type**. You can choose only from parent object types for the **Child Type** object type that you selected.

You can define multiple parent associations to replicate to newly created objects.

9. Click **Done**.

Results

If both **Folder Filter** and **Filter Rules** are provided, the filters are combined with an AND statement. An object must match both filters to be available for selection.

Adding a Delete action

Define an action as **Delete** to delete child objects that are associated with an object that is open in a Task View.

About this task

The delete action is available only in grid relationship fields. The **Relationship Type** must be Children.

The delete action deletes selected objects. It is not used to disassociate objects. Use an associate action to provide a means of disassociating child objects from an object that is open in a Task View.

The user must have access permissions that allow them to delete objects.

Procedure

1. In a grid relationship field, click **Add Action** and choose **Delete**.
2. Enter a **Label**. It displays as a button label. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

3. Click **Done**.

Adding a Get Watson Suggestion action

Define an action as **Get Watson Suggestion** to specify a field to make object association suggestions.

About this task

For more information, see [“Adding a classifier field that makes object association suggestions” on page 430](#).

Defining dynamic filters on actions in relationship fields

You can use **Filter Rules** to add dynamic filters to actions in grid and card relationship fields.

About this task

You can use a dynamic filter on an action when you want to reduce the number of related objects that a user can choose from and ensure that the list is appropriate for the object that is open. For example, in a Task View for Risk objects, when a user clicks **Select Controls** and a Grid View opens, you might want to show a list of related controls that are in the same risk category as the Risk object that is open.

The filter is dynamic in the sense that the related objects that are listed in a Grid View are determined when the view is actually used.

Dynamic filters work only:

- For the **Associate**, **Associate Primary Parent**, or **Copy Recursive** actions.
- For direct (parent and child) relationships.

When you define a **Filter Rule**, you set up a field pair. The field pair consists of a field on a related object and a field on the object for the view. The system compares the values in the two fields to determine whether there is a match for the filter. The two fields can either both be text fields or both be enumerated fields. If the two fields are enumerated fields, they can both be single value, both be multivalued, or be mixed. You can define multiple filter rules. All filter rules are combined with an AND statement.

Dynamic filters do not support the comparison of empty values. If an object has an empty value for the field that is defined in the **Filter Rule**, the rule is ignored.

For more information about rules, see [“Configuring rules” on page 439](#).

On the JSON tab, filter rules are defined in a *filterRules* element in an actions section if *actionType* is *associate*, *associatePrimary*, or *copyRecursive*.

Procedure

1. In a card or grid relationship field, click **Add Action** and choose **Associate**, **Associate Primary Parent**, or **Copy Recursive**.
2. In **Filter Rules**, click **Add Rule**. Establish the field pair that the rule is based on.
 - a) Choose a field in **[object type] field value**. You can choose only from fields on the related object type that is specified in the relationship field. For example, if you are defining a Task View for a Risk object and building a relationship field for a SOXControl object, this field displays as **Control field value**. You can choose only from fields on a SOXControl object.
 - b) Leave **Equals** as is. It cannot be changed.
 - c) Choose a value in **[object type] field value**. You can choose only from fields on the object type for the view and only matching field types for the first field in the field pair. For example, if you are defining a Task View for a Risk object and building a relationship field for a SOXControl object, this field displays as **Risk field value**. You can choose only from fields on a Risk object and only field types that match the field type of the field given in **Control field value**.
 - d) Click **Done**.
 - e) Add more filter rules (optional).
3. Click **Done**.

Configuring rules

The Task Focused UI includes a framework of rules for field dependencies and validation. Rules ensure that the data that users enter in the Task Focused UI is valid.

A rule can either provide additional validation of a field's value or alter the behavior of a field, such as hiding a field. Some rules allow you to compare the value of a field with another field, while others compare it to values defined in the rule itself.

Rules are available in Creation and Task Views but not in Grid Views. In Task Views, you cannot add rules to fields in the Task View header. Controller fields used in rules must be in the view.

To define rules, go to the **Design** tab in the View Designer. Select a field and click **Add Rule** in a field's property panel. Select a **Rule Type** and add conditions. The field type determines what rule types are available. A field can have multiple rule types.

To remove a rule, hover over the rule on the property panel. Click remove and then **Done**.

When you open the property panel for a field, the field type and field definition in the Standard UI determines whether **Required** and **Read Only** properties are displayed. The properties might be hidden entirely, might be read only, or might be toggles that you can set.

There are also **Required**, **Editable**, and **Read Only** rule types. These rule types are defined when you click **Add Rule**. Use them to define whether a field is required, editable, or read only based on the value of another field in the view, called a *controller* field.

- If **Required** is displayed as a toggle, you can set it to True. In which case, the **Required** rule type is disabled. If you set it to False, you can define a **Required** rule type that determines whether the field is required.
- If **Read Only** is displayed as a toggle, you can set it to True. In which case, the **Editable** and **Read Only** rule types are disabled. If you set it to False, you can define **Editable** or **Read Only** rule types that determine whether the field is read only or editable.

Note: Dependent picklists are not defined in Task or Creation views. However, the views enforce the dependent pick lists that are defined on object types. For more information, see [“Adding and working with dependent picklists \(Task Focused UI\)”](#) on page 289.

Table 152. Rule Types

Design	JSON	Description
Editable Read Only	<i>editable</i> <i>readOnly</i>	Makes a field editable or read-only based on the value of one or more other fields.
Visible Hidden	<i>visible</i> <i>hidden</i>	Makes a field visible or hidden based on the value of one or more other fields.
Required	<i>required</i>	Makes a field required based on the value of one or more other fields. In a view, the Save button is disabled until the field is given a value.
Greater than Greater than or equal Less than Less than or equal Equal	<i>greater</i> <i>greaterEqual</i> <i>less</i> <i>lessEqual</i> <i>equal</i>	Validates that a field's value is greater than, less than, or equal to the value of another field of the same type, or to a value provided in the rule definition. You can define these rules on integer, decimal, date, or currency fields. In a view, a red star is displayed next to the field and the Save button is disabled until the validation passes. The rules can also validate that two text fields have the same value.
Minimum Length Maximum Length	<i>minLength</i> <i>maxLength</i>	Validates that the value of a text field has a minimum or maximum number of characters. In a view, the Save button is disabled until the validation passes. You can define these rules on string fields.
Pattern	<i>pattern</i>	Validates that the value of a text field has a specified format, for example, nnn-nn-nnnn. In a view, the Save button is disabled until the validation passes. You can define this rules on string fields.

Defining Editable and Read Only rules

The **Editable** and **Read Only** rule types make a field editable or read-only depending on the value or values of one or more controller fields in a view.

About this task

You can define **Editable** and **Read Only** rules on any field type.

If an Editable field dependency is already defined on a field in the Standard UI, you cannot define additional rules of these types on that field in a Task or Creation View.

The controller fields must be either enumeration or actor fields.

When a field is made read-only because of a change to a controller field, changes to that field's value since it was last saved are reverted to its original value.

Note: An exception exists for changes to values in grid and card relationship fields. The values cannot be reverted because they are saved immediately.

On the JSON tab, editable and read only rules are defined when *type* is set to *editable* or *readOnly*. Must also specify either a *controllers* or *controllerName* attribute. Specify one or more *controllers* as an array. Use the short-hand format *controllerName* rather than *controllers* to specify only a single *controller* for which ANY value will satisfy the rule's criterion.

In the steps below, select **Editable** or **Read Only** in **Rule Type**.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the field that you want to add a rule to.
3. In the property panel, click **Add Rule**.
4. Select a **Rule Type**.
5. In **Controlled By**, choose **One field with any value** or **Multiple controllers or values**.
6. If you choose **One field with any value**:
 - a) Select a **Controlling Field**.
 - b) Click **Done**.
7. If you choose **Multiple controllers or values**:
 - a) In **Controlling Field Logic** select **All controlling field conditions must be met** or **Any controlling field condition may be met**.
 - b) Click **Add Controller Field**.
 - c) Choose a field in **Controlling Field**. All available controlling fields are displayed. The next selections depend on the field type.
 - For actor fields, you can set **Match Current User** and/or select other users or user groups in **Other Users or Groups**. Any match on either field resolves the controller to true. If **Match Current User** is set to true, the signed on user must be the user or be in a user group for the value in the **Controlling Field**.
 - For enumerated type fields, click **Values** and you can choose one or more individual values.
 - Click **Done**.
 - d) Add **Add Controller Field** to add the next controller field. Repeat the previous steps. Continue until all controller fields have been added. Although you can change the order of the controller fields, it has no effect in the view.
8. Click **Done**.

Defining Visible and Hidden rules

The **Visible** and **Hidden** rule types make a field or inline guidance for sections either visible or hidden depending on the value or values of one or more controller fields in a view.

Before you begin

About this task

The **Visible** and **Hidden** rule can be defined on any field type and on inline guidance for sections. If a visible field dependency is already defined on a field in the Standard UI, you cannot define additional rules of these types on that field in a Task or Creation View.

The *controllers* must be either enumeration or actor fields.

When a field is made hidden because of a change to a controller field, changes to that field's value since it was last saved are reverted to its original value.

Note: An exception exists for changes to values in grid and card relationship fields. The values cannot be reverted because they are saved immediately.

On the JSON tab, visible and hidden rules are defined when *type* is set to *visible* or *hidden*. You must specify either a *controllers* or *controllerName* attribute. For more information, see [“Defining Editable and Read Only rules”](#) on page 440.

In the following steps, select **Visible** or **Hidden** in **Rule Type**.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the field that you want to add a rule to.
3. In the property panel, click **Add Rule**.
4. Select a **Rule Type**.
5. In **Controlled By**, choose **One field with any value** or **Multiple controllers or values**.
6. If you choose **One field with any value**:
 - a) Select a **Controlling Field**.
 - b) Click **Done**.
7. If you choose **Multiple controllers or values**:
 - a) In **Controlling Field Logic** select **All controlling field conditions must be met** or **Any controlling field condition may be met**.
 - b) Click **Add Controller Field**.
 - c) Choose a field in **Controlling Field**. All available controlling fields are displayed. The next selections depend on the field type.
 - For actor fields, you can set **Match Current User** and/or select other users or user groups in **Other Users or Groups**. Any match on either field resolves the controller to true. If **Match Current User** is set to true, the signed on user must be the user or be in a user group for the value in the **Controlling Field**.
 - For enumerated type fields, click **Values** and you can choose one or more individual values.
 - Click **Done**.
 - d) Add **Add Controller Field** to add the next controller field. Repeat the previous steps. Continue until all controller fields have been added. Although you can change the order of the controller fields, it has no effect in the view.
8. Click **Done**.

Defining Required rules

The **Required** rule type makes a field required depending on the value or values of one or more controller fields in a view.

About this task

The field is validated to make sure that it has a value any time a change is made to the field or one of its controller fields. If the field is required but is missing a value, a message is displayed on the field and the **Save** button is disabled.

This rule can be defined on any field type, except on relationship fields where the object type (*objectTypeName* in JSON) is set to SOXDocument.

If a required field dependency is already defined on a field in the Standard UI, you cannot define additional rules of this type on that field in a Task or Creation View.

The controllers must be either enumeration or actor fields.

On the JSON tab, a required rule is defined when *type* is set to `required`. You must specify either a *controllers* or *controllerName* attribute. See [“Defining Editable and Read Only rules” on page 440](#) for more details.

In the following steps, select **Required** in **Rule Type**.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the field that you want to add a rule to.
3. In the property panel, click **Add Rule**.
4. Select a **Rule Type**.
5. In **Controlled By**, choose **One field with any value** or **Multiple controllers or values**.
6. If you choose **One field with any value**:
 - a) Select a **Controlling Field**.
 - b) Click **Done**.
7. If you choose **Multiple controllers or values**:
 - a) In **Controlling Field Logic** select **All controlling field conditions must be met** or **Any controlling field condition may be met**.
 - b) Click **Add Controller Field**.
 - c) Choose a field in **Controlling Field**. All available controlling fields are displayed. The next selections depend on the field type.
 - For actor fields, you can set **Match Current User** and/or select other users or user groups in **Other Users or Groups**. Any match on either field resolves the controller to true. If **Match Current User** is set to true, the signed on user must be the user or be in a user group for the value in the **Controlling Field**.
 - For enumerated type fields, click **Values** and you can choose one or more individual values.
 - Click **Done**.
 - d) Add **Add Controller Field** to add the next controller field. Repeat the previous steps. Continue until all controller fields have been added. Although you can change the order of the controller fields, it has no effect in the view.
8. Click **Done**.

Defining Greater than, Greater than or equal, Less than, Less than or equal, and Equal rules

The **Greater Than**, **Greater than or equal**, **Less than**, **Less than or equal**, and **Equal** rule types validate the value of a field and make sure that it satisfies the condition applied by the rule type. The rule can be set up to compare a field's value with the value of another field of the same type, or with a value defined in the rule itself.

About this task

Any time a change is made to the field it is validated to make sure that it satisfies the condition. If the value is being compared to another field, it is validated any time that field's value changes. If the condition is not satisfied, a message is displayed on the field and the **Save** button is disabled. The message explains how to provide a valid value.

These rule types can be set up on integer, decimal, date, and currency fields. When comparing two fields, both fields must be of the same type. If one of the fields has no value, the rule is not evaluated.

Text fields can also have an Equal rule, but only to compare against another text field.

On the JSON tab, comparison rules are defined when *type* is set to `greater`, `greaterEqual`, `less`, `lessEqual`, or `equal`. A *compareTo* attribute must also be specified.

Procedure

1. In the View Designer, click the **Design** tab.

The palette is displayed.

2. Select the field that you want to add a rule to.
3. In the property panel, click **Add Rule**.
4. In **Rule Type**, choose **Greater Than**, **Greater than or equal**, **Less than**, **Less than or equal**, or **Equal**.
5. In **Compare To**, the field type determines the options.
 - For integer, decimal, and currency fields, you can choose **A specific value** and enter a value. Do not include quotation marks, decimal separators, currency codes, or symbols.
 - For integer, decimal, currency, date, and text fields, you can choose **Another field** and select a field. Only fields in the view and of the same field type are listed.
 - For currency fields, values are compared using the base amount rather than the local amount. This allows values to be compared across different currency codes.
 - For date fields, you can compare the value to today and optionally add an offset in days.

Because the value of **Today** changes as time progresses, rules that compare against **Today** are evaluated only when a user selects a value for the field. This prevents previously saved data from failing validation due to the changing nature of **Today**.
6. Apply a **Severity** (optional). For information, see [“Controlling error severity on rules” on page 445](#).
7. Click **Done**.

Defining Minimum Length and Maximum Length rules

The **Minimum Length** and **Maximum Length** rule type validates the length of a text field or, if used together, defines a range.

About this task

The field is validated to make sure that the length of the text value is valid any time a change is made to the field. If the condition is not satisfied, a message is displayed on the field and the **Save** button is disabled. The message states how many characters are allowed.

These rules can be set up only for text fields.

You can provide either the **Minimum Length** or **Maximum Length** rule type. You can apply both to define a range.

On the JSON tab, minimum and maximum rules are defined when *type* is set to `minLength` or `maxLength`. Specify *compareTo* as a number of characters within quotation marks.

Procedure

1. In the View Designer, click the **Design** tab.

The palette is displayed.
2. Select the field that you want to add a rule to.
3. In the property panel, click **Add Rule**.
4. In **Rule Type**, choose **Minimum Length** or **Maximum Length**.
5. Enter the number of characters.
6. Apply a **Severity** (optional). For information, see [“Controlling error severity on rules” on page 445](#).
7. Click **Done**.

Defining Pattern rules

The **Pattern** rule type validates that a text field has a specified format.

About this task

The field is validated to make sure that the value has the correct format any time its value is changed. If the format is not correct, a message is displayed on the field and the **Save** button is disabled.

This rule can only be set up for text fields.

On the JSON tab, a pattern rule is defined when *type* is set to *pattern*. Specify *compareTo* as a valid regular expression.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the field that you want to add a rule to.
3. In the property panel, click **Add Rule**.
4. In **Rule Type**, choose **Pattern**.
5. In **Pattern**, enter a valid regular expression, for example, `^[0-9]{3}-[0-9]{2}-[0-9]{4}$`.
6. Apply a **Severity** (optional). For information, see [“Controlling error severity on rules” on page 445](#).
7. Click **Done**.

Controlling error severity on rules

Use the **Severity** property to control whether errors or warnings are issued when users enter values that do not pass validation rules.

About this task

When users enter values that do not pass a field's validation rules, an error is issued and the object cannot be saved. However, if you apply the **Severity** property, warnings are issued rather than errors. When a warning is issued, an object can still be saved.

You can add a **Severity** property to any validation rule type (**Greater Than**, **Greater than or equal**, **Less than**, **Less than or equal**, and **Equal**). You can specify it to be an error, warning, or information. If a rule has no severity property, errors are issued.

For example, a warning can be issued if a date field is not within the next 90 days. If the *severity* property is omitted, an error is issued.

The text in the message is set by the system and cannot be customized.

Multiple warning messages can be displayed for a field. However, only one error message is displayed.

Conditions, for example, field dependencies and field attributes, that are defined in the Standard UI always issue errors rather than warnings.

An information message behaves like a warning but is displayed with an information symbol. The error message text is the same whether it is a warning or an information.

On the JSON tab, specify *severity* as *error*, *warning*, or *info*.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the field that you want to add a rule to.

3. In the property panel, click **Add Rule**.
4. In **Rule Type**, choose a rule type.
5. In **Severity**, choose **Error**, **Warning**, or **Info**.
6. Click **Done**.

Customizing the Primary menu

You can customize the Primary menu in the Task Focused UI so that you can quickly access the object types you work on most frequently.

- You can change the order of object types in the Primary menu and its submenus.
- You can add object types to a submenu.
- You can add a submenu that contains object types.

In the Task Focused UI, the menu items that are displayed depend on the user's profile and role template, and the configuration of the menu in Settings.

You cannot add system items, such as My Background Processes or Administration, to the Primary menu.

If you use IBM Cognos Analytics, the **Analytics** menu item displays as the first item in the list. This placement cannot be changed.

If OpenPages is used with IBM OpenPages for IBM Cloud Pak for Data, the **Analytics** menu item does not display on the Primary menu.

The changes that you make also impact the navigation bar in the Standard UI. For example, if you add a new top-level item to the Primary menu, it is displayed as a new tab on the navigation bar in the Standard UI.



Warning: The changes that you make might be lost when you upgrade IBM OpenPages with Watson. Like all customizations, include these changes when you back up your environment before an upgrade.

Changing the order of menu items

You can change the order of object types in the Primary menu and its submenus.

Procedure

1. Click  > **System Configuration** > **Settings**.
2. Click **Applications** > **Common** > **Configuration** > **Show Hidden Settings** and set the value to true.
3. Click **Applications** > **GRCM** > **NavigationMenu**.
4. To change the order of top-level items, edit the **Items** setting under **NavigationMenu**. Change the order of items in the comma-separated list.

Note: The following items are not displayed in the Task Focused UI:
MyOpenPages, Reports, IncidentManagement, Administration

For example, if you move Vendors after Organization, the Primary menu looks like this:

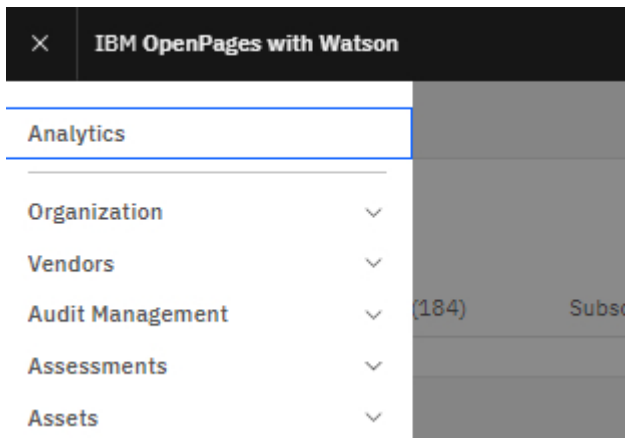


Figure 46. Reordering menu items

You might need to refresh the page or log out and log in to see your changes.

5. To change the order of items in a submenu, expand the folder for the submenu, and then edit the **ObjectTypes** setting.

For example, suppose that you want **Contracts** to be the first item in the **Vendors** submenu. To do this, expand the **Vendors** folder, click the **ObjectTypes** setting, and put Contract first in the list of object types. The Primary menu looks like this:

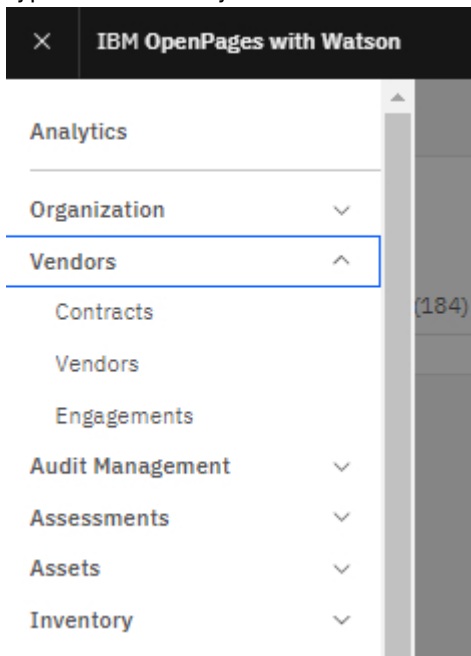


Figure 47. Reordering menu items

You might need to refresh the page or log out and log in to see your changes.

Results

The Primary menu is updated. The navigation bar in the Standard UI is also updated.

Adding object types to a submenu

You can add object types to a submenu in the Primary menu.

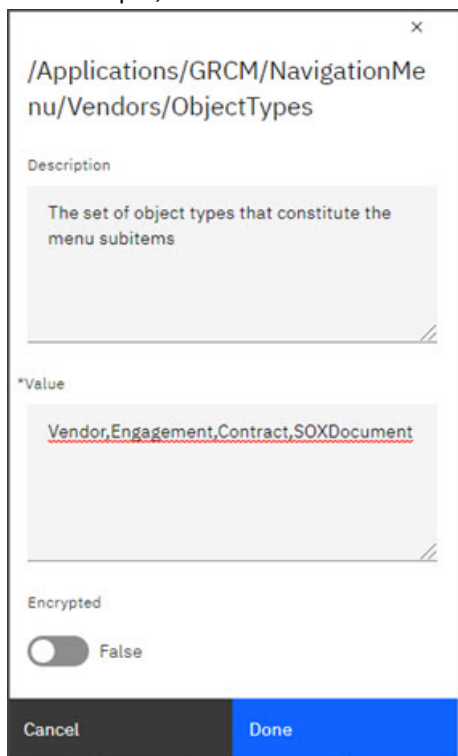
Procedure

1. Click  > **System Configuration** > **Settings**.
2. Click **Applications** > **Common** > **Configuration** > **Show Hidden Settings** and set the value to `true`.
3. Click **Applications** > **GRCM** > **NavigationMenu**.
4. Expand the folder where you want to add the object types.

For example, if you want to add an object type to the **Vendors** submenu, expand the **Vendors** folder.

5. Edit the **ObjectTypes** setting. Add the object types to the comma-separated list, in the order in which you want them to appear.

For example, to add **Files** to the **Vendors** submenu, add `SOXDocument` to the list.



The screenshot shows a configuration window titled `/Applications/GRCM/NavigationMenu/Vendors/ObjectTypes`. It contains a description: "The set of object types that constitute the menu subitems". Below this is a text field labeled `*Value` containing the text `Vendor,Engagement,Contract,SOXDocument`. At the bottom, there is an "Encrypted" toggle switch set to "False". The window has "Cancel" and "Done" buttons at the bottom.

Figure 48. Adding SOXDocument to the ObjectTypes setting

The Primary menu looks like this:

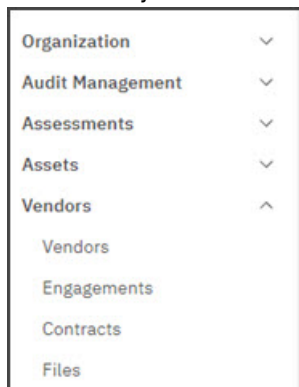


Figure 49. Adding Files to the Vendors menu

You might need to refresh the page or log out and log in to see your changes.

Note: If you don't see the object, check the **Applications > GRCM > NavigationMenu > Administration > Schema > SpecialObjectTypes > ObjectTypes** setting. If the object is listed, remove it.

Results

The Primary menu is updated. The navigation bar in the Standard UI is also updated.

Creating a new top-level menu item

You can add a top-level menu item that contains object types.

Procedure

1. Click  > **System Configuration > Settings**.
2. Create an application text string for your new top-level menu.
See [“Adding new keys” on page 576](#).
For example, create an application text string called `Test` and set its default value to `Files & Links`.
3. Click **Applications > Common > Configuration > Show Hidden Settings** and set the value to `true`.
4. Click **Applications > Common > Configuration > Allow Create and Delete Settings** and set the value to `true`.
5. Click **Applications > GRCM**.
6. Click the check box next to the **NavigationMenu** folder, and then click **Add Folder**. Type a folder name.
Users do not see the folder name in the user interface.
For example, create a folder called `TestFolder`.
7. Refresh the page.
The folder that you created is now visible.
8. Click the check box next to the new folder that you created in step 6. Click **Add Setting**.
9. Add a setting called `ObjectTypes` and set the value to a comma-separated list of object type names
For example: `SOXDocument,SOXExternalDocument`
10. Add another setting. Name it `TextKey` and set its value to the application text string that you created in step 2.



Figure 50. Adding the application text string for the new submenu

11. In the **Items** setting under **NavigationMenu**, add the name of the folder that you created. Put the folder name in the order where you want it to display in the Primary menu.

For example, add `TestFolder` after `Organization`.

The Primary menu looks like this:

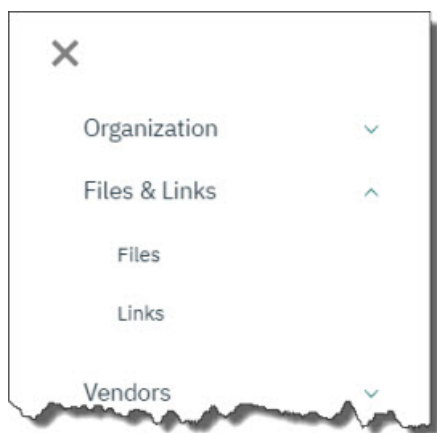


Figure 51. Adding the submenu

Remember: The submenu name is defined by the application text string that you created in step 2. If you're following the examples, you see Files & Links, the value of the Test application text string.

You might need to refresh the page or log out and log in to see your changes.

Results

The Primary menu is updated. The navigation bar in the Standard UI is also updated.

Configuring a Net Promoter Score (NPS) survey

Configure a Net Promoter Score survey so that users can send feedback about OpenPages to IBM.

Before you begin

Ensure that your firewall allows users access to the survey. Review the URL to Medallia, the Net Promoter Score survey provider. For more information, see [“Reviewing the Net Promoter Score \(NPS\) survey settings” on page 619](#).

About this task

If a Net Promoter Score survey is enabled, users are presented with two possibilities to complete a survey:

- An NPS Feedback button
- An NPS survey form on log in

An NPS Feedback button is always displayed on the Home page for users who are eligible to receive a survey. Users can provide feedback at any time and as often as they want.

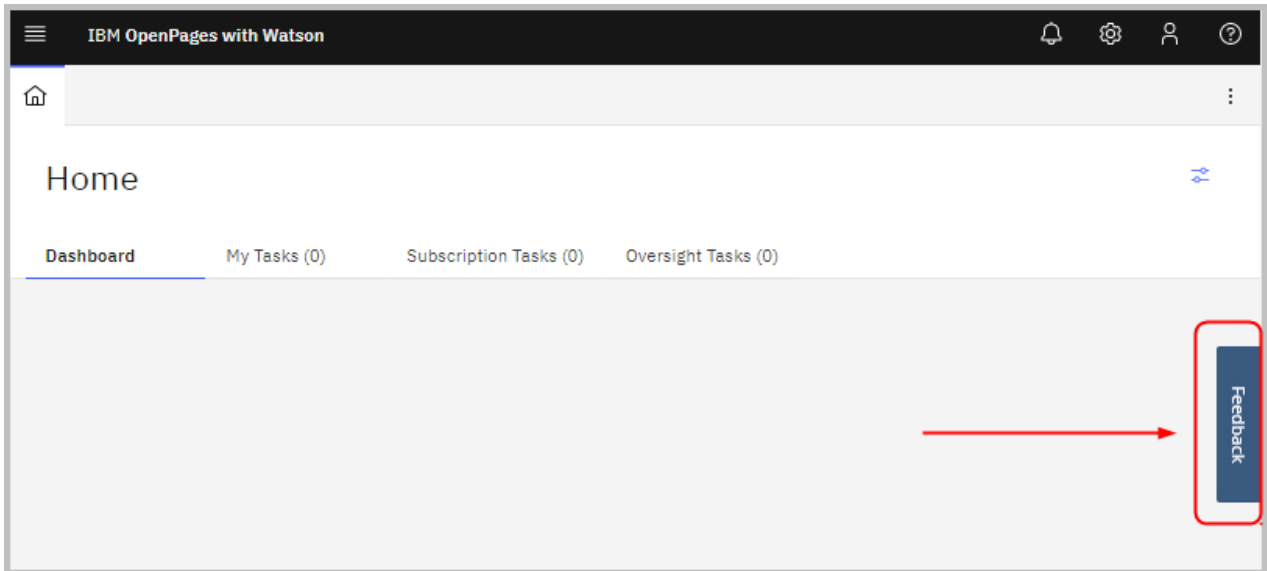


Figure 52. NPS Feedback button on the Home page

An NPS survey form is displayed on log in to users who meet the following conditions:

- The user must be eligible to receive the survey, as defined in **Included Users or Groups** and **Excluded Users or Groups**.
- The user must meet the Medallia frequency requirements:
 - The user was last presented with a survey at least 90 days ago. This prevents the survey from being presented too frequently. It is presented regardless of whether the user provided feedback or declined to provide feedback on the last survey.
 - The user must have logged in at least 30 days ago. This prevents the survey from being presented to brand new users.

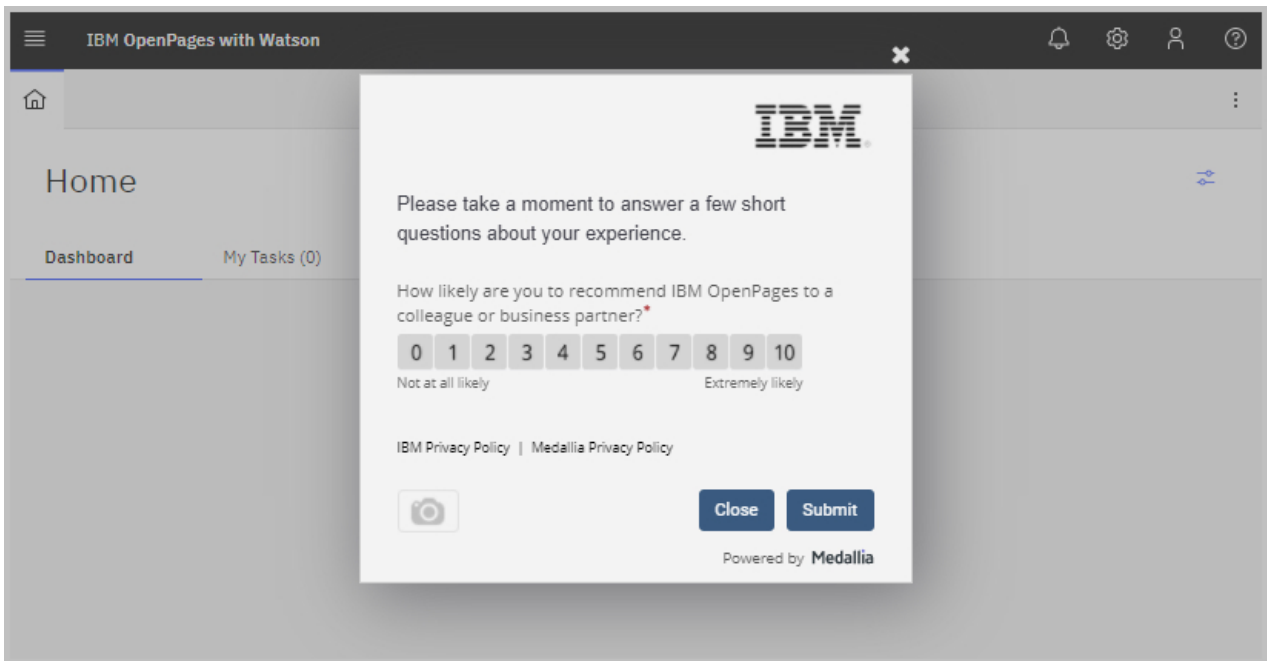


Figure 53. NPS survey form displayed after logging in

Procedure

1. Click  > **Integrations** > **NPS Settings**.
Or, in 8.2.0.3 and earlier, click  > **System Configuration** > **NPS Settings**.
2. Set **Enable User Feedback Survey** to true. The default is false.
3. Enter your **IBM Customer Number** (ICN).
4. Set **Percentage of Users to Target** to light (15%), medium (50%), or heavy (100%).
5. In **Included Users or Groups**, build the group of users who are eligible to receive a survey. If empty, all users are eligible to receive a survey.
6. In **Excluded Users or Groups**, add the users or groups who explicitly never receive a survey.
7. Click **Submit**.

Exporting and importing dashboards

You can migrate dashboards from one environment to another environment using Export Configuration and Import Configuration.

Before you begin

Read Chapter 26, “Migrating OpenPages environments,” on page 865 to ensure that you are familiar with how to use Export Configuration and Import Configuration.

About this task

Dashboards are exported or imported as part of the profile that they belong to.

You can migrate dashboards that have been defined per profile by an administrator with the  > **System Configuration** > **Dashboards** task.

When you export dashboards using Export Configuration, the dashboards for the profiles you select are exported to a migration file.

Panels that users have manually added to their dashboard are excluded.

An alternative to using Export Configuration and Import Configuration is to use the ObjectManager tool. For more information, see [“Migrating configuration changes” on page 911](#).

Procedure

1. Follow the instructions described in [“Exporting configuration items from the source environment \(Task Focused UI\)” on page 873](#) and choose the profiles to export.
2. Follow the instructions described in [“Importing a migration file \(Task Focused UI\)” on page 877](#) to import the migration file into a target environment.
3. Access and test the dashboards in the target environment. Verify that the content of the dashboards is correct.

Themes

Themes are used to customize the colors that are displayed in the Task Focused UI. Users can apply a theme by using the  > **Change Theme** task.

There are two types of themes:

- System themes
- Custom themes

System themes

There are four system themes, listed from lightest to darkest:

- Carbon White
- Carbon Gray 10 (default)
- Carbon Gray 90
- Carbon Gray 100

The system themes have defined colors. Carbon White and Carbon Gray 10 are light themes, while Carbon Gray 90 and 100 are dark themes.

The system themes are associated with two palettes:

- Categorical Palette
- Monochromatic Palette

Palettes contain colors that you can apply to enumerated string fields and numeric field ranges in charts and in views in the View Designer.

The colors in the system themes and the palettes cannot be changed.

Custom themes

Administrators can create their own themes, called custom themes. Initially, a custom theme must be based on an existing theme. Then you can design the theme and apply colors that meet your needs. You can, for example, apply colors that identity your company's color palette. Custom themes can be the default, enabled, disabled, and deleted.

Custom themes do not include their own palettes. Custom themes that are based on a light theme are combined with colors from the light set of colors in the Categorical Palette. Custom themes that are based on a dark theme are combined with colors from the dark set of colors in the Categorical Palette. For more information about applying colors to fields, see [“Supported color palettes for field values” on page 409](#).

Carbon

Colors in the system themes and the palettes used in OpenPages are based on Carbon. For more information, see <https://www.carbondesignsystem.com/guidelines/color/overview>.

IBM Watson Assistant

If IBM Watson Assistant is used, a selected theme is automatically applied to the chat bot.

Theme list

Use the  > **System Configuration** > **Themes** task to work with themes.

The Theme List shows themes that are defined in the Task Focused UI. From the Theme List, you can:

- Click a theme. The theme opens and you can view it or make changes.
 - A system theme can be enabled, disabled, or designated as the default. Otherwise, no changes are allowed. They cannot be deleted.
 - A custom theme can be enabled, disabled, deleted, designated as the default, and colors can be changed.
- To change the default theme, select **Default**. It is not possible to clear the **Default** check box on a theme, instead, mark another theme as the default. Only one theme can be the default.

- To enable a theme, select **Enabled**. All enabled themes are displayed to users for selection on the  > **Change Theme** task. Enable only one theme to not allow users to change the theme. There is no application permission for the  > **Change Theme** task.
- Select the check box next to a single theme or multiple themes to update numerous themes. The bulk update options are:
 - Delete
 - Enable
 - Disable
 System themes cannot be deleted.
 Clear the check boxes to hide the bulk update options.
- Click **Add Theme** to create a new theme. For more information, see [“Defining custom themes” on page 454](#).
- Click the **Name** column header to change the sort order of the list.

Users apply themes

After themes have been configured, users can click  > **Themes** and apply a theme. Any system or custom theme that is enabled is available for selection. The default theme is applied if they do not apply a theme.

Restrictions

The following restrictions exist for themes:

- Theme selection is retained the next time a user signs in, regardless of browser.
- Themes are not applied to:
 - The login page. The login page always uses the Carbon Gray 10 theme.
 - The page header and menus. They are always black/white.
 - Questionnaires.
 - Helpers.
- Themes are not supported on Microsoft Internet Explorer 11 . In this case, Carbon Gray 10 theme is applied.

Defining custom themes

Custom themes contain a color scheme that is designed for your organization.

Before you begin

Decide what existing system or custom theme is the base for the new custom them.

To do this task, you need the **SOX > Administration > Solutions** application permission.

About this task

Design the theme and apply colors that meet your needs.

Table 153. UI components	
UI component	Defines the color of the ...
interactive-01	Bar above a tab and the background color for buttons like Add New.

Table 153. UI components (continued)	
UI component	Defines the color of the ...
interactive-03	Contrast and tertiary buttons
interactive-04	Check marks in a Grid View.
text-04	Text in buttons like Add New.
link-01	Text in clickable links, for example, the names in a Grid View list.
focus	Elements that show where the cursor is, for example around an X box.
hover-primary	Color of elements as you hover over elements
active-primary	Background color of elements as you make selections, for example, the background color of the menu bar when you select an item in a Grid View for bulk actions.
hover-primary-text	Color of text as as you hover over elements
hover-tertiary	Color of tertiary hover
active-tertiary	Color of active tertiary elements

Procedure

1. Click  > **System Configuration** > **Themes**.
2. Click **Add Theme**.
3. Select a them in **Base Theme**.
The colors of the base theme are applied as a preview. Select a different base theme, if needed.
4. Enter a **Name**. Make it meaningful. It is displayed to users in the  > **Change Theme** task.
5. Enter a **Description**.
6. Leave **Enabled** cleared.
7. In **Colors** click a UI element and apply a color.
 - Click a color on the color model, or
 - Click the drop down. The options depend on the browser you use. For example, for Chrome, there are options to provide color values as RGB, HSL, and HEX.
8. Repeat the previous step for each UI element.
9. Click **Done**.

What to do next

Test the theme, make adjustments as needed, and enable it. After the custom theme is enabled, it is available to users to apply.

Chapter 14. Configuring GRC Calculations

Use the GRC Calculations feature to automatically set values on fields when an object is created, calculation input fields are updated, object associations are made, or a **run a calculation** workflow action starts.

Setting up GRC Calculations

Configure GRC Calculations so that calculations can be used in OpenPages.

About this task

During the configuration process, complete the following tasks to prepare for implementing GRC Calculations in OpenPages.

Procedure

1. Update the permissions for role templates for administrators who are configuring the calculations.
 - a) Click **Administration > Role Templates > <role template> > Role Permissions**.
 - b) Select the **SOX > Administration > Calculation** permission.

Administrators with this permission enabled can define calculations with **Calculations** on the **Administration** menu in the Task Focused UI. They can also access and run calculations from **Calculations**.
2. Review the registry settings that apply to calculations. They are located in the **Platform > Calculation** registry settings folder. Especially review:
 - **Enabled**

Calculations are enabled (true|false).
 - **Always Recalculate on the Object Save**

Recalculate object fields on the save operation all the time (true|false). If false, object fields are recalculated only when the input fields are updated.

The other registry settings control concurrent jobs and how asynchronous processing is handled. They are: **Async Enabled**, **Async Polling Period**, **Async Queue Builder Only**, and **Concurrent Calculation Jobs**. Additionally, the **Platform > Processes > Bulk run calculations > Transaction Timeout** registry setting is used when an administrator runs a calculation. For more information, see [“Running a calculation as an administrator”](#) on page 490.
3. Optional: Customize the content of email notifications that are sent when an administrator runs a calculation. You can use the default email template or customize the text to meet your requirements. For more information, see [“Customizing email notifications for GRC Calculations”](#) on page 492.
4. Define, test, and implement calculations. For more information, see [“Defining a calculation”](#) on page 467.

What to do next

Complete the following prerequisites:

- Review the Task Views in the Task Focused UI. Review whether input fields and set fields are displayed in the Task Views so that you understand how users experience calculations and calculated values. For more information, see [“Defining a Task View”](#) on page 394.
- Review the GRC Workflow feature in OpenPages. Review what workflows are setting field values. For more information, see [“Defining a workflow action that sets fields”](#) on page 539.

Calculation fundamentals

The GRC Calculations feature is based on calculation definitions.

Calculations are defined by using the  > **Solution Configuration** > **Calculations** task. After you publish a calculation, it is available in OpenPages.

Show me how

This video shows you how to use the **Calculations** task. It explains the fields in a calculation definition and how a list of operations is constructed.

<https://youtu.be/0MZy60Clr-U>

Calculation definitions

A calculation definition is defined for one object type. An object type can have multiple calculations.

A calculation definition has the following characteristics:

- A calculation definition is static.
- A calculation definition is versioned.

Each time a calculation definition is published, a new version of that calculation definition is made available to users. The new version is used for object changes that are made after it is published. It does not affect calculations that have already been run.

- A calculation definition can be disabled.

When a calculation definition is disabled, no new calculation can be run. Disabled calculation definitions can be re-enabled.

A calculation definition is made up of the following elements:

- Calculation properties

Calculation properties define basic information, for example, the object type that the calculation applies to and whether the calculation is enabled.

- Applicability conditions

Applicability conditions restrict the calculation to objects that meet specific criteria.

- Operations

Operations determine what the calculation does.

Goal of a calculation

The goal of a calculation is to set a value for one or more fields on an object, based on the values of one or more other fields. Only fields on the object type for the calculation can be set. Fields on related object types cannot be set.

Operations determine what a calculation does

A calculation is made up of multiple operations. A calculation can have three types of operations:

- Input field operation

Retrieves an input field that is used in a later operation. An input field operation can be from the current object, a related object, or the Preference object. Conditions can be defined on the input field. A calculation can have multiple input field operations.

- Variable operation

Contains an intermediary value that is used in a later operation. A variable operation contains an expression that can use all previously defined operations, be they input fields, other variables, or set field operations. A calculation can have multiple variable operations.

- Set field operation

Sets a field value on an object. A set field operation contains an expression that can use all previously defined operations, be they input fields, variables, or other set field operations. A calculation can have multiple set field operations.

Operations are defined for a single calculation. They cannot be shared among multiple calculations.

What does the calculation type do?

The calculation type determines whether a calculation can be started by a workflow. There are two calculation types:

- Manual calculations are started only by a **run a calculation** action in a workflow.
- Automatic calculations are started in all other ways except by a **run a calculation** action in a workflow.

In Task Views, fields that contain the result of an automatic calculation are read only and cannot be changed by the users. However, fields that contain the result of a manual calculation are not read only and the values can be changed by users.

When do calculations run?

A calculation runs when an enabled, published calculation exists for an object type. An object must meet both a calculation's applicability and conditions on the value of the input field, if defined.

Manual calculations run when a **run a calculation** action in a workflow starts.

Automatic calculations run when the following actions take place:

- A user creates an object. The calculation runs if the object is created in either the Task Focused UI or the Standard UI.
- A user updates a calculation's input field on an object in a Task View in the Task Focused UI or a view in the Standard UI.
- A user updates a calculation's input field on a related object in a Task View in the Task Focused UI or a view in the Standard UI. If a user updates an input field on, for example, a child object, a calculation on a parent object type is run.
- A user associates an existing related object to another object, where either or both objects contain an input field that is used in a calculation. The association can occur in either the Task Focused UI or the Standard UI.
- A user starts a workflow that creates an object for an object type that has a calculation.
- A user completes a stage in a workflow that updates a calculation's input field that is used in a calculation.
- A user completes a stage in a workflow that updates a calculation's input field on a related object.
- A user completes a stage in a workflow that associates an existing related object to another object, where either object contains an input field that is used in a calculation.
- An administrator runs a calculation by using the  > **Solution Configuration** > **Calculations** task. The administrator selects a single calculation and clicks .
- An administrator uploads data with Fast Map in either the Task Focused UI or the Standard UI. The data contains new objects or changes to a calculation's input fields.
- Data is loaded by using an API, where the data contains new objects, changes to a calculation's input fields (on the object or related objects), or changes to object associations.

When a user updates an input field on an object in a Task View, all calculations for that object type that use the changed input fields are run. The order that the calculations run cannot be defined.

New calculations and existing objects

When you create a new calculation, it does not automatically run on existing objects. A calculation is run when actions described in [“When do calculations run?”](#) on page 459 take place.

Object types and calculations

An object type can have multiple calculations. But each calculation must set different fields. No two calculations can set the same field. A calculation runs for all objects that qualify for it, given the applicability and input field conditions.

Debugging calculations

For information about correcting calculations that have errors, see [“Testing and debugging a calculation”](#) on page 491.

Sample calculations

OpenPages includes the following sample calculations:

- Business Continuity BIA Scoring

Determines Impact Score using requirements, financial impacts, and reputation impacts. Uses Impact Score to determine Impact Tier and Maximum Acceptable Outage.

- Risk Rating

Calculates the Inherent Risk Rating and Residual Risk Rating based on defined registry keys.

- Loss Event

Calculates the Net Loss, Recovery Amount, Gross Loss, and Estimated Gross Loss based on the underlying Loss Impact and Loss Recovery.

- Resource CIA

Calculates the resource criticality based on the high watermark for CIA (confidentiality, integrity, and availability).

Comparison of calculations and triggers

The GRC Calculations feature, together with the GRC Workflow feature, provide a powerful platform that allows organizations to tailor the system to their specific requirements. Existing OpenPages customers that use triggers can make a plan to transition from triggers to GRC Calculations and GRC Workflow.

Calculations can replace the following functionality that was previously available in triggers:

- Automation for data input
- Mathematical operations
- Assessment rating assignments
- Data aggregation
- Helper links

Calculations and workflows that are defined by using GRC Calculations and GRC Workflow are easier to define and maintain than triggers. Triggers require a high level of technical expertise, whereas most calculations and workflows can be defined by business specialists. For complicated calculations and workflows, technical expertise is an advantage.

Triggers that currently work in your environment, continue to work. But your organization should make a plan to transition existing triggers to calculations.

Functionality that is available in triggers is also available in GRC Calculations and GRC Workflow.

GRC Calculations FAQs

The following list provides answers to frequently asked questions about calculations.

Can one calculation set values for multiple fields?

Yes. A single calculation can set the values for multiple fields. They must be fields on the object type that the calculation is defined for.

Can multiple calculations set a value for the same field?

Yes. A field can be used as a set value operation in multiple calculations. However, the order in which calculations run is not guaranteed. Therefore, plan your calculations to avoid collisions and overwrites.

Can a calculation set a value for the same set value field multiple times within that calculation?

Yes. A value can be set multiple times for the same field within a calculation (this means that multiple set field operations for the same field are allowed).

Are there fields that a calculation is not allowed to set?

Yes. A calculation is not allowed to set the values for computed fields, workflow system fields, and many of the system fields like System Fields:Creation Date. Additionally, calculations cannot set fields that are defined as relationship fields in Task Views in the Task Focused UI.

Can a calculation set user and date system fields?

No. While a calculation can use the user and date system fields as input fields, a calculation cannot set the value of the following system fields:

- System Fields:Created By
- System Fields>Last Modified By
- System Fields.Last Modification Date
- System Fields.Creation Date
- System Fields:Name

If you create your own user field and want to set it to the value in, for example, System Fields>Last Modified By, be sure to define the user field with field type defined as simple string and display type as user selector.

Can a calculation set a field that is defined as read-only in a Task View?

Yes.

Do calculations honor field dependency rules?

No. For example, if a user updates the value of an input field on a Task View and a calculation runs, the object can be saved even if the output field value does not meet the field dependency rules.

What happens if a calculation updates a controlling field?

Use caution when defining calculations that set values for fields that are controlling fields. In some situations, changes can be lost in Task Views because a loop is created. For example, say that Field B is a controlling field and Field A is a dependent field (is set to Read-only or Editable based on Field B). If a calculation updates Field B based on a change to Field A, the update to Field A might be lost in the Task view. The dependency is enforced without saving the updated value.

To avoid this, use separate Task Views, one that runs a calculation and one that sets dependent fields.

Do calculations honor dependent pick list rules if a calculation is based on the controlling field ?

Yes. If a calculation sets a value for a field that is a controlling field in a dependent pick list, it also sets values for dependent fields to allowed values.

Can a calculation set a field on a related object or Preference object?

No. A calculation can set a field only on objects of the object type that the calculation is defined for.

Can a calculation be based on a field on a related object or Preference object?

Yes. A calculation can use fields on a related object or Preference object as input fields.

Can one calculation be linked to another calculation?

No, each calculation is independent. But the result of one calculation can cascade to other calculations. For more information, see [“Designing a calculation” on page 463](#).

Can I include a filter within a calculation?

Yes, a filter (condition) can be applied to input fields that are defined for related objects and Preference objects.

Can a calculation get invoked from a workflow?

Yes, if the workflow starts an action that causes a calculation to run. This might include creating an object, updating an input field on an object, updating an input field on a related object, and associating objects.

Can I access siblings on a calculation?

No. Fields from siblings of the open object cannot be used as input fields.

Can I access child, parent, ascendent, and descendant objects?

Yes, input fields can be fields from child, parent, ascendent, or descendant objects.

Can a calculation invoke an association or copy operation?

No. A calculation can only set field values.

Can a calculation access the values in registry settings?

Yes

Are there sample calculations?

Yes.

Can I access a specific value in a multi-value field?

Yes. Use an index on the field, for example, `at([$Causal Category$], 2)`, to access the enumerated value in the third position of the Causal Category field. It accesses the third position because counting begins at zero.

Can I edit the text in the body of the email that is sent to the administrator after they run a calculation?

Yes. The body text is defined in application text.

Is there an undo for a calculation?

No.

Can calculations be included in the scheduler?

No.

Can calculations be started by a workflow action?

Yes. Manual calculations can be started by a **run a calculation** operation on a workflow action. For more information, see [“Defining a workflow action that runs a calculation” on page 544.](#)

Can I schedule a calculation to run in off hours?

No. However, you can disable calculations all together or disable individual calculations to control when calculations run. For example, you can disable calculations before a Fast map load. Then, run the calculations after the data is loaded. You can also disable calculations during working hours. Enable the calculations, run them in off hours, and disable them again during working hours.

Does a calculation run if I change an input field in the Standard UI?

Yes, calculations are triggered by changes to data in the database, regardless of whether the change is initiated in the Task Focused UI, the Standard UI, API, FastMap, and so.

Must the input fields and set fields be included in a Task View for a calculation to run?

No. Calculations are run when an input field is changed, regardless of whether it is shown in a Task View or not. If the input field is required, it must be in the creation view.

When I use a Task View, what causes a calculation to run?

A calculation runs either when an object is saved or only when an input field that is used in a calculation is changed. The **Always Recalculate on the Object Save** registry setting controls the behavior.

Why are set fields updated BEFORE I click Save in a Task View?

When you change an input field and move the focus outside the field, all the calculations that use that input field are run in preview mode. The new values for set fields are calculated and displayed if they are included in the Task View. The values that are shown in preview mode are saved to the database when you click **Save**.

Do I have to click Save for the calculation to run?

No. Calculations run in preview mode when you move the focus outside an input field whose value you changed. But you must click Save for the results of the calculation to be saved in the database.

Can I manually update the value in a set field in a Task View, thereby overriding the calculated value?

It depends on the calculation type. Set fields that are calculated by automatic calculations are read only in a Task View. If the calculation is disabled, the set field becomes editable or however the field is defined to display in the Task View. Set fields that are calculated by manual calculations are not read only in a Task View and are editable.

What can I do to optimize speed and performance?

Keep the expressions as simple and short as possible. A calculation with many operations with complex expressions might impact performance.

Designing a calculation

Designing a calculation involves knowing what result the calculation should achieve, understanding the input fields and field values, the field value that is set, and understanding what is possible in the calculation expression.

Know what objects the calculation applies to

A calculation can run for all or selected objects of an object type.

If a calculation is run for only selected objects, the applicability and input field conditions on the calculation define the selection criteria.

Part of testing a calculation is to verify that the applicability and input field conditions are defined correctly.

Know the calculation result

Know the result that the calculation should achieve.

Know whether the calculation is started by a workflow

Calculation type (automatic or manual) determines whether a calculation can be started with a **run a calculation** action in a workflow.

Understand the operations in a calculation

Understand the operations in a calculation.

Use input fields and variables in a calculation. It makes the calculations modular and easier to debug.

Add comments to the expression.

Follow good programming practices.

Study the Loss Event calculation to see how the result of one set field operation can be used in subsequent operations.

Understand the calculation expression

Understand the possibilities available in the calculation expressions. For more information, see [“Expressions in GRC Calculations” on page 471](#).

Understand how a calculation can cascade to other calculations

Each calculation is independent. But the result of one calculation can cause a cascade effect to other calculations.

The following example illustrates how this works:

1. A change is made to Input Field A that is used in Calculation A, which sets Set Field A to a value.
2. Set Field A is an input field that is used in Calculation B. When Set Field A changes, Calculation B runs. Calculation B sets Set Field B to a value.
3. Set Field B is an input field that is used in Calculation C and Calculation D. When Set Field B changes, Calculation C and Calculation D run. Calculation C sets Set Field C to a value. Calculation D sets Set Field D to a value.
4. The calculation can continue this pattern.

Keep it simple

Calculations that have many operations that have complex expressions can impact performance. Avoid making a calculation overly complicated. Keep the expressions as short and simple as possible.

Common calculation use cases

Study the use cases to learn how to write calculations for common scenarios you might encounter.

- Use case 1: Set a value on a parent object that is the sum of values on child objects
- Use case 2: Set a date on a parent object based on dates from child objects
- Use case 3: Set an enumerated value based on other enumerated values

Use case 1: Set a value on a parent object that is the sum of values on child objects

In this use case, you want to set Estimated Gross Loss on Loss Event parent objects to the sum of Estimated Loss on the child Loss Impact objects. The calculation is defined for the Loss Event object type. The two fields that are involved are OPSS-LossEv:Estimated Gross Loss on Loss Event objects and OPSS-LossIm:Estimated Loss on Loss Impact objects.

The Estimated Loss operation gets the values of the OPSS-LossIm:Estimated Loss field from the child Loss Impact objects.

Table 154. Use Case 1: Estimated Loss operation				
Operation Name	Type	Object Type	Field	Reference type
Estimated Loss	Input Field	LossImpact	OPSS-LossIm:Estimated Loss	Direct Child

The Set Estimated Loss operation sums the values of the OPSS-LossIm:Estimated Loss field from the Estimated Loss operation and sets the value of OPSS-LossEv:Estimated Loss on the parent object to the sum or to zero.

Table 155. Use Case 1: Set Estimated Loss operation

Operation Name	Type	Output Field	Expression
Set Estimated Loss	Set Field	OPSS-LossEv:Estimated Loss	if exists (SUM ([\$Estimated Loss\$]))then SUM ([\$Estimated Loss\$]) else currency(0.00, 'USD') endif

Use case 2: Set a date on a parent object based on dates from child objects

In this use case, you want to set a Due Date on a parent Issue to the most recent due date on child Action Item objects. The calculation is defined for the Issue object type. The two fields that are involved are OPSS-AI:Due Date on Issue objects and OPSS-AI:Due Date on Action Item objects.

Table 156. Use case 2: GetDate operation

Operation Name	Type	Object Type	Field	Reference type
GetDate	Input Field	SOXTask	OPSS-AI:Due Date	Direct Child

Table 157. Use Case 2: Set Date operation

Operation Name	Type	Output Field	Expression
SetDate	Set Field	OPSS-Iss:Due Date	max ([\$GetDate\$])

Use case 3: Set an enumerated value based on other enumerated values

In this use case, you want to set Criticality on Resource objects to values from Confidentiality, Integrity, and Availability on the same object. The calculation is defined for the Resource object type.

The first three operations get the values of the OPSS-CIA:Confidentiality, OPSS-CIA:Integrity, and OPSS-CIA:Availability fields on a resource object.

Table 158. Use Case 3: the three Input Field operations

Operation Name	Type	Object Type	Field	Reference type
C	Input Field	Resource	OPSS-CIA:Confidentiality	Self
I	Input Field	Resource	OPSS-CIA:Integrity	Self
A	Input Field	Resource	OPSS-CIA:Availability	Self

The Set Criticality operation sets the value of OPSS-CIA:Criticality based on the values of the three preceding operations.

Table 159. Use Case 3: Set Criticality operation

Operation Name	Type	Output Field	Expression
Set Criticality	Set Field	OPSS-CIA:Criticality	<pre> If ([C\$] == 'High' OR [I\$] == 'High' OR [A\$] == 'High') then 'High' elif ([C\$] == 'Medium' OR [I\$] == 'Medium' OR [A\$] == 'Medium') then 'Medium' elif ([C\$] == 'Low' OR [I\$] == 'Low' OR [A\$] == 'Low') then 'Low' else 'Not Available' endif </pre>

Managing calculation definitions

The **Calculations** task is used to define, publish, and manage calculations.

To manage calculations, click  > **Solution Configuration** > **Calculations**. Whether the menu item is displayed depends on your access permissions.

Calculation List

When you click  > **Solution Configuration** > **Calculations**, a Calculation List is displayed.

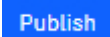
From the Calculation List, you can:

- Click a calculation. The calculation definition opens and you can view or make changes to it.
- Click the **Name** column header to change the sort order of the list.
- Select the check box next to a single calculation or multiple calculations to update numerous calculations. The bulk update options are:
 - Enable
 - Disable
 - Delete
- Select the check box next to a single calculation and click  to run a calculation for numerous objects at once. For more information, see [“Running a calculation as an administrator” on page 490](#).
- Click **Add New** to create a new calculation. For more information, see [“Defining a calculation” on page 467](#).

How to save a calculation

Your work is automatically saved as you define a calculation.

How to publish a calculation

Click  when the calculation is finished.

Each time a calculation definition is published, a new version of that calculation definition is made available.

How to discard a draft version of a calculation

To discard changes you made to a calculation, click **Discard Draft**. All changes since the last published version are discarded.

How to disable a calculation

To disable a calculation, select a calculation from the Calculation List. Select **Disable**.

How to work on a calculation as a team

When you have a calculation definition open, the URL contains the calculation's internal name. If you are working on the calculation with colleagues, you can send them the URL to share your progress. Although you can collaborate with colleagues, only one user should work on a calculation at a time.

Defining a calculation

A calculation definition contains basic information, applicability, and operations.

About this task

The main parts of a calculation are the operations and the expressions. Operations determine what the calculation does:

- At a minimum, one **Set Field** operation is mandatory.
- A calculation can optionally have multiple **Input Field** operations and multiple **Variable** operations.
- The operations are processed in the order listed. The operations can be reordered.
- Place the **Set Field** operations last in the list.
- An expression must be valid and free of syntax errors to save an operation.

Tip: If you are having trouble getting the syntax correct for an expression, provide a dummy expression like 1+2 so that you can save the operation and not lose your work if the session times out.

Procedure

1. Click  > **Solution Configuration** > **Calculations**.
2. Click **Add New**.
3. Enter an internal **Name** for the calculation.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

4. Enter a **Description**.

Note: For complicated calculations, provide a short statement that describes each operation. This ensures that anyone who follows you can understand and debug the calculation.

5. Leave **Enabled** selected. It can be changed later.
6. Select an **Object Type**. It cannot be changed later.
7. Select Manual or Automatic in **Calculation Type**.

- Manual calculations are started only by a **run a calculation** action in a workflow.
- Automatic calculations are started in all other ways except by a **run a calculation** action in a workflow.

8. Click **Add**.

The window expands. The word *Draft* and the version number, *1*, are displayed next to the calculation name. You can begin defining the calculation.

9. In **Applicability** you define the conditions for the calculation. Expand **Applicability** and click **Add Condition**. The **Applicability** panel opens.

- Leave **Applicability** empty if the calculation runs for all objects of the object type.
- Add conditions to restrict the calculation to specific objects of the object type.
- For each condition, you build a comparison statement with two fields and an operator.
- If you define multiple conditions, all conditions must be met for the calculation to start.

To override this rule, define **Advanced Logic** to combine the conditions in a specific way.

a) In **Compare** you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is (or is not) a specified user or is (or is not) in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

b) In **Using** choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

c) In **To** you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**.

- **An expression**

Enter a single field or variable from the list in “Using variables, functions, and fields ” on page 503. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).

- Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
 - **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

Note: An object's system comment field (System Fields:Comment) cannot be used in a field comparison in a condition.
- d) If you chose a date field in **Compare**, you can optionally define an offset in **Adjust Date By**.
- **A specified value** and enter **Number of Days**.
 - **A field in the current object**
 - **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
 - **A field in the Preference object**

You can optionally add **Filter By** conditions.
- e) Click **Done**.
- The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.
- f) Optional: Add more conditions.
- g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.
- The order of operations is: () then NOT then AND then OR.
- For example:
- 1 or 2 or 3
 - 1 and (2 or 3)
 - 1 not (2 or 3)
10. In **Operations** you define what the calculation does. Expand **Operations** and click **Add Operation**. The **Operation** panel opens.
11. Define **Input Field** operations for the calculation.
- a) Click **Add Action**.
 - b) In **Type**, select Input Field.
 - c) Enter an internal **Name** for the operation.
 - d) Click **Add Field**.

The panel expands and three options are displayed:

 - **A field in the current object**
 - **A field in a related object**
 - **A field in a Preference object**
 - e) If you select **A field in the current object**, select an **Object Field** and click **Done**.

f) If you select **A field in a related object**, complete the following fields:

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Select a field in **Related Object Field**.
- Choose a **Field to sort on**.
- Select Ascending or Descending in **Sort Direction**.

An example of how you can use sorting is to list months in different orders. For example, to analyze trends, you might want to sort KRI values by January, February, and March. Then, later by March, February, and January.

- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
- Add **Filter By** conditions (optional). If you add multiple conditions, set **Advanced Logic** as needed.
- Click **Done**.

g) If you select **A field in a Preference object**, complete the following fields:

- Select a field in **Preference Object Field**.
- Add **Filter By** conditions (optional). If you add multiple conditions, set **Advanced Logic** as needed.
- Click **Done**.

h) Define more **Input Field** operations, as needed by the calculation.

12. Define **Variable** operations for the calculation.

- a) Click **Add Action**.
- b) In **Type**, select Variable.
- c) Enter an internal **Name** for the operation.
- d) All input fields, variables, and set fields that precede this operation are listed in **Involved Fields**.
- e) Enter an **Expression**. For more information, see [“Expressions in GRC Calculations” on page 471](#).
- f) Click **Done**.
- g) Define more **Variable** operations, as needed by the calculation.

Tip: If

13. Define **Set Field** operations for the calculation.

- a) Click **Add Action**.
- b) In **Type**, select Set Field.
- c) Enter an internal **Name** for the operation.
- d) Select a field in **Output Field**.
- e) All input fields, variables, and set fields that precede this operation are listed in **Involved Fields**.
- f) Enter an **Expression**. For more information, see [“Expressions in GRC Calculations” on page 471](#).
- g) Click **Done**.
- h) Define more **Set Field** operations, as needed by the calculation.

14. Review the operations.

- a) To reorder the operations, click [Reorder ↑↓](#).
Use drag and drop to set the processing order. Click **Done**.
- b) To remove an operation, click it and select **Remove**.

15. When you are ready to test the calculation, click **Publish**.

The 1 version of the calculation becomes the first published version.

16. Run the calculation to test it.

For information about correcting calculations that have errors, see [“Testing and debugging a calculation”](#) on page 491.

17. If you need to make changes to the calculation, open it again. Since you are now opening a published calculation, the word *Published* appears, the version number is displayed next to the calculation name and the **Publish** button is grayed out. When you make a change to the calculation, *Published* changes to *Draft*, the version number is incremented by 1, and the **Publish** button becomes active.

What to do next

Each time you change the calculation, you need to publish it and re-test it.

Expressions in GRC Calculations

The Set Field and Variable operations in a calculation contain an **expression**.

Syntax rules for expressions

An expression must be written in the correct syntax.

Syntax rules:

- Numbers, dates, string values, operands, object fields, operation names, variables, and functions are allowed.
- String values must be enclosed in single or double quote marks. For variables such as [`$END_USER$`] string values enclosed in double quote marks are resolved, whereas those enclosed in single quote marks are kept as-is.
- Spaces are not a syntax error between operands in an entire expression, for example, between operands like `+` and `==` and in `if/then/else/endif` statements. Extra spaces and no spaces are allowed.
- Carriage returns (new lines) are allowed.
- Values within [`$$`] are case-sensitive. This means that the special variable, [`$END_USER$`], must be written in uppercase in an expression.
- Values outside of [`$$`] are case-insensitive. This means that the names of functions are case-insensitive, for example, `sum`, `Sum`, and `SUM` are all valid.
- String values that are enclosed in single or double quote marks are case sensitive. For example, for an `if/then/else/endif` statement that contains a condition like `if "test" == "TEST"`, the result is false.
- Operation names must be enclosed in [`$$`] and be given correctly in both spelling and case. This means that an operation that is named `Get Due Date` is written in subsequent operation expressions as [`$Get Due Date$`].
- Object field names must be given in the following format: [`$field group:field name$`]. The field group and field name must be given correctly in both spelling and case.
- Object field names that reference parent, child, and preference objects must be given in the correct format. The object type, field group, and field names must be given correctly in both spelling and case. For example, for [`$Child:object type/field group:field name$`], the spelling and case of all names must be correct and the C in `Child` must be capitalized.

For more information about object fields, see [“Object fields”](#) on page 477.

- Add system variables, if needed. For more information, see [“System variables”](#) on page 478.
- Apply functions, if needed. Functions must be correct for the data type. For more information, see:

- [“Functions for string values” on page 479](#)
- [“Functions for lists and numerical values” on page 481](#)
- [“Functions for dates” on page 483](#)
- [“Functions for currency values” on page 485](#)
- Arguments for functions must be enclosed in parentheses.
- Starting and ending parentheses must match.
- Functions that require no arguments must have empty parentheses. For example, the `tomorrow` function is written as `tomorrow()`.
- A function can contain another function as an argument.
- Use `if/then/else/endif` statements, if needed. For more information, see [“If/then/else/endif statements” on page 486](#).
- Add comments (optional). Comments must be given in the correct format.

Operands for string values

The `+` operand can be used on string values.

Table 160. Operands for string values			
Operand	Description	Expression	Result
+	Concatenates two or more text strings. A string value can be enclosed in either single or double quotation marks.	"abc" + "def" [\$S1\$] + [\$S2\$], where the operations contain the string values abc and def [\$S1\$] + "def" [\$field group:field name\$] + "def", where the field contains string value abc	abcdef

Operands for numerical values

The following operands can be used for integer, decimal, or currency values. Add and subtract can be used for dates. If an argument is a list, the operand is applied to all items in the list.

Table 161. Operands for numerical values			
Operand	Description	Expression	Result
+	Add	100.00 + 5 [\$N1\$] + [\$N2\$], where N1 contains 100.00 and N2 contains 5 [\$N1\$] + 5 [\$field group:field name\$] + 5, where the field contains 100.00 ([\$TODAY\$] + 10), where today is May 18, 2020.	105.00 105.00 105.00 105.00 2020-05-28
-	Subtract	100.00 - 5	95.00

Table 161. Operands for numerical values (continued)

Operand	Description	Expression	Result
		[\$field group:field name\$] - 5, where the field contains the date 2020-06-06	2020-06-01
		[\$L1\$] - 5, where L1 is a list of the following values: 100.00, 200.00, 300.00	95.00, 195.00, 295.00
*	Multiply	100.00 * 5	500.00
/	Divide	100.00 / 5	20.00
()	Set precedence	100.00 / (2 + 3)	20.00
		10 * ([\$N1\$] - 30.3), where N1 contains 100.00.	697.00

Syntax rules for comments

You can add two types of comments to an expression:

- Paragraph comments

Enclose the text in slash single or double asterisk, for example, /* text */ or /** text */. Optionally begin each line within the block with an asterisk.

- One-line comments

- Begin a line with double slash, for example, // text
- Place the comment text after an expression, for example, [\$N1\$] + 5 // Add 5 to N1

Both types of comments are included in the following example expression:

```
/**
 * KRI Indicator trend
 * Calculated by comparing two KRI Value Breach Status and setting to Not Determine, Steady,
 * Worse, Better
 */
//case 1: not enough KRI values
if count([$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescB:OPSS-KRIVAL:Value
Date$]) < 2
// case 2: one of the recent has "Not Determine"
elif (( at ([$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescB:OPSS-KRIVAL:Value
Date$], 0)
== ( at ([$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescB:OPSS-KRIVAL:Value
Date$], 1)
// case 3: two recent ones have the same breach status
```

Tutorial: writing expressions

The tutorial illustrates how to write expressions in different ways.

Show me how

This video shows you how to write expressions that use integer, decimal, and currency fields. You also learn how to use parentheses for precedence and how to apply operands to lists and dates.

<https://youtu.be/CfPCYZX10AM>

Basic expressions

Let's start with some basic expressions, where the operation type is Variable.

Table 162. Examples of basic expressions			
Operation name	Expression	Result	Note
N1	1 + 2	N1 is set to 3	
D1	2020-10-10 + 2	D1 is set to 2020-10-12	
S1	"abc" + "def"	S1 is set to abcdef	

Expressions that use operation names

Then, to use those operations in expressions in subsequent operations, enclose the operation name in [\$], as shown in the following examples:

Table 163. Examples of expressions that use operation names		
Expression	Result	Note
([\$N1\$] * 2)+100	106	Where N1 contains the expression, 1 + 2
[\$D1\$] + 10	2020-10-22	Where D1 contains the expression, 2020-10-10 + 2
[\$S1\$] + [\$S2\$]	abcdefxyz	Where S1 and S2 contain the string values <i>abcdef</i> and <i>xyz</i> , respectively

Expressions that use object fields

Expressions can retrieve values from object fields, as shown in the following examples:

Table 164. Examples of expressions that use object fields		
Expression	Result	Note
[\$Field Group:Number1\$] + [\$Field Group:Number2\$]	3	Where the value in <i>Number1</i> is 1 and <i>Number2</i> is 2
[\$Field Group:Date1\$] + 2	2020-10-12	Where the value in <i>Date1</i> is 2020-10-10
[\$Field Group:String1\$] + [\$Field Group:String2\$]	abcdefxyz	Where the value in <i>String1</i> is <i>abcdef</i> and <i>String2</i> is <i>xyz</i>

Expressions that mix operation names and object fields

You can mix operation names and object fields in an expression, as shown in the following examples:

Table 165. Examples of basic expressions that mix operation names and fields names		
Expression	Result	Note
[\$N1\$] * [\$Field Group: Number3\$]	300	Where <i>Number3</i> contains 100.
[\$D1\$] + 10	2020-10-22	Where [\$D1\$] contains the expression, 2020-10-10 + 2
[\$S1\$] + [\$Field Group: Description\$]	abcdefDescription value	Where [\$Field Group: Description\$] contains <i>Description value</i>

Expressions that use functions

You can apply functions to values, fields, and operations, as shown in the following examples:

Table 166. Examples of functions that are applied to values, fields, and operations.		
Expression	Result	Note
max(5000, 10000, 15000, 20000)	20000	The max function finds the maximum value in a list.
max ([\$Child: LossImpact/ OPSS- LossIm: Estimated Loss\$])	20000.00	Where four child objects contain the following values in the Estimated Loss field: 5000.00, 10000.00, 15000.00, 20000.00
max ([\$Loss1\$], [\$Loss2\$], [\$Loss3\$], [\$Loss4\$])	20000.00	Where the four operations that are given contain the following values: 5000.00, 10000.00, 15000.00, 20000.00
count ([\$Child: LossImpact/ OPSS- LossIm: Estimated Loss\$])	4	Number of items

Working with lists

Lists are a means to access and work with multiple values for objects and fields.

Show me how

This video shows you how to work with lists. It explains how to retrieve values from related objects fields, work with multi-valued fields, create and manipulate lists, and apply functions to items in a list.

<https://youtu.be/6TPd1sXeH5k>

About lists

A common requirement for a calculation is to get values from multiple objects and do something with the list of values that is retrieved.

To get the values from multiple objects, define an Input Field operation that designates what object type and field you want to retrieve. You can optionally apply a condition to get only specific values. For more information, see [“Applying a condition to get only specific objects in a list” on page 477](#). You can also optionally sort the values in ascending or descending direction either by the chosen field or another field on the object type.

The result of such an Input Field operation is a list of values.

For example, for a calculation on the Loss Event object type, the Estimated Loss operation retrieves values in the OPSS-LossIm:Estimated Loss field on all child LossImpact objects. If there are four child objects, the result is like this:

```
5000.00, 10000.00, 15000.00, 20000.00
```

If the list were sorted in descending order, it would be:

```
20000.00, 15000.00 10000.00 5000.00
```

Expressions in subsequent operations can refer to the Estimated Loss operation and apply functions either to the entire list or individual items in the list using an index. The term *index* refers to positions in the list, where the index starts counting at zero. In the previous example, the value 20000.00 is in index position 0, 15000.00 is in position 1, and so on.

The same principle applies if an Input Field operation retrieves values from a field that contains multiple values, for example, a multi-actor field. You can optionally apply a condition to get only specific values. You can also optionally sort the values in ascending or descending direction either by the chosen field or another field on the object type.

Some functions can be applied to all items in a list, regardless of the type of data in the list. For example, the count function can be used for any list. Given the previous example, the result of the following two example expressions is 4.

```
count ([$Estimated Loss$])
```

```
count ([$Child:LossImpact/OPSS-LossIm:Estimated Loss$])
```

Some functions can be applied to lists of specific data types. For example, for a list that contains numerical values, you can use the sum, max, and min functions.

For example, a Set Field operation can contain this expression that sets Estimated Gross Loss on the parent Loss Event to sum of the results in the Estimated Loss operation:

```
if exists (SUM ([$Estimated Loss$]) )then SUM ([$Estimated Loss$]) else currency(0.00, 'USD')
```

The result of the Set Field operation would be 50000.00 (20000.00 + 15000.00 + 10000.00 + 5000.00).

For a list that contains string values, you can use functions that split, join, and concatenate string values.

Some functions use the index so that you can access specific positions in the list, for example, you can use the at function to access specific items in a list. For example, if the Estimated Loss operation results in the following list:

```
5000.00, 10000.00, 15000.00, 20000.00
```

The following expression results in 5000.00, the value of the item in the first position (index position zero).

```
at ([$Estimated Loss$], 0)
```

The following expression results in 15000.00, the value of the item in the third position (index position two).

```
at ([$Estimated Loss$], 2)
```

You can also add and remove items from the list. For example, the following expression appends items to a list:

```
append( [$Estimated Loss$], 30000.00, 40000.00, 50000.00 )
```

Results in the following list:

```
5000.00, 10000.00, 15000.00, 20000.00, 30000.00, 40000.00, 50000.00
```

Applying a condition to get only specific objects in a list

You can optionally apply a condition to get only specific objects in a list. For example, say that for a calculation on Risk objects, you want to get a count of child Control objects. But you only want to count Control objects whose Operating Effectiveness is set to Effective. Define an input field named GetControls for Control objects and specify a **Filter By** condition where Operating Effectiveness is equal to Effective. Then define an operation with the expression count ([\$GetControls\$]). The result is a count of Control objects whose Operating Effectiveness is set to Effective.

Setting an Output Field value when the expression result is a list

Special rules apply when an expression result is a list of values but the Set Field operation contains an Output Field that sets a single field value.

Table 167. List results in expressions	
When an expression result is...	Output Field is set to ...
One related object	The field value from that object
Multiple related objects but they all have the same field value	The value from the objects
Multiple related objects, where only one object has a value and the others are not set	The value from the one object
Multiple related objects, where they have different values	No value is set and a calculation error is issued.

Object fields

Object fields can be used in expressions.

Object fields are relative to the object type of the calculation and the current object, meaning the object that the calculation is processing.

Table 168. Syntax for object fields		
For	Use the syntax	Result
An object field on current object	[\$field group:field name\$]	The value of an object field on the current object.
A system field on the current object	[\$System Fields:field name\$]	The value of a system field on the current object.
A field on the Preference object	[\$Preference/field group:field name\$]	The value of an object field on the Preference object type.

Table 168. Syntax for object fields (continued)		
For	Use the syntax	Result
Fields on parent objects	<code>[\$Parent:object type/field group:field name\$]</code>	A list of field values from parent objects, relative to the current object.
Fields on child objects	<code>[\$Child:object type/field group:field name\$]</code>	A list of field values from child objects, relative to the current object.
Fields on child objects and sort the list in ascending or descending order	<code>[\$Child:object type/field group:field name/AscBy:field group:sort field name\$]</code> <code>[\$Child:object type/field group:field name/DescBy:field group:sort field name\$]</code>	A sorted list of field values from child objects, relative to the current object.

The following examples illustrate how you can use object fields:

Table 169. Examples of expressions that use object fields		
Expression	Result	Note
<code>[\$Child:SOXTask/System Fields:Name\$]</code>	Iss-11-001-AI_01, Iss-11-001-AI_02, Iss-11-001-AI_03, Iss-11-001-AI_04	Result is a list of the names of all child Action Items objects on a parent Issue object
<code>[\$Child:LossImpact/OPSS-LossIm:Estimated Loss\$]</code>	5000.00, 10000.00, 15000.00, 20000.00	Result is a list of estimated loss values from child Loss Impact objects for a parent Loss Event object

System variables

System variables can be used in expressions.

Table 170. System variables	
System variable	Result
<code>[\$APPLICATION_URL\$]</code>	A URL for OpenPages.
<code>[\$COGNOS_URL\$]</code>	A URL for Cognos Analytics.
<code>[\$ApplicationText/application text key\$]</code>	Application text content.
<code>[\$System Fields:Task View URL\$]</code>	A URL to an object task view.
<code>[\$Setting/OpenPages/....\$]</code>	A registry setting value.
<code>[\$END_USER\$]</code>	The user name of the signed on user.
<code>[\$TODAY\$]</code>	Today's date.

Table 170. System variables (continued)	
System variable	Result
[\$DaysFromNowDategiven\$]	A day count from today to a given date. Requires one argument (a date field). [\$DaysFromNow/field group:field name\$] For example: [\$DaysFromNow/OPSS-Iss:Original Due Date\$] result is 15, given that there are 15 days between today and the Issue Due Date

The following examples illustrate how you can use system variables:

Table 171. Examples of expressions that use system variables		
Expression	Result	Note
[\$END_USER\$]	JSMITH	Result is the user name of the signed on user.
format ([\$END_USER\$])	Jane Smith - JSMITH	Result is <first name + last name - user name> of the signed on user.
[\$TODAY\$]	2020-11-09	Given that today's date is November 9, 2020.
format ([\$TODAY\$]+10)	November 19, 2020	Given that today's date is November 9, 2020.
[\$Setting/OpenPages/Solutions/PCM/Global Settings/Draft Policy Library\$]	Global Financial Services	The result is the value of the Draft Policy Library registry setting, in this case, Global Financial Services.

Functions for string values

Functions for string values can be used in expressions.

Table 172. Functions for string values		
Function	Description	Syntax
format	Result is a value that is changed to human-readable format. Valid for date, currency, and actor fields. For example, use format to make a date human readable so that it can then be appended to a text string. Use format to make an actor field human readable so that a user's name can be inserted in a text string. Do not use format for a date subject to an equation.	format(input) Example: format([\$fdGroup1:fdDate1\$]) or format([\$fdGroup1:fdCurrency1\$])

Table 172. Functions for string values (continued)

Function	Description	Syntax
indexOf	Result is the index of the first occurrence of <i>string2</i> out of <i>string1</i> . It is used to get parts of a string. If <i>string1</i> is a list, the indexOf function is applied to all items in the list. The result is a list of integers.	indexOf(<i>string1</i>,<i>string2</i>) Example: indexOf('abcdefedcba', 'c') result is 2
join	Joins a list of strings, where <i>delimiter</i> is a delimiter. For example, use to build a list of child action item names separated by commas.	join(<i>delimiter</i>,<i>list1</i>) Example: join('-', ['a', 'b', 'c']) result is a-b-c
LastIndexOf	Result is the index of the last occurrence of <i>string2</i> out of <i>string1</i> . If <i>string1</i> is a list, the LastIndexOf function is applied to all items in the list. The result is a list of integers.	LastIndexOf(<i>string1</i>,<i>string2</i>) Example: lastIndexOf('abcdefedcba', 'e') result is 6
length	Result is the length of a string value. For example, if you know the length, you can use it in an expression to remove part of a string. If <i>string1</i> is a list, the length function is applied to all items in the list.	length(<i>string1</i>) Example: length('abcdef') result is 5
substring	Result is a portion of a string. The portion can either be from a given start index position to the end of the string or from given start and end index positions. Can have one or two arguments. If one argument is given, the result is a string value from the given index position to the end of the string. If two arguments are given, result is the portion of a string between the index positions. For example, if a unique identifier is part of an object name that was assigned using autonaming, use substring to extract the positions that contain the identifier. If <i>list1</i> is itself a list, the substring function is applied to all items in the list. The result is a list of substring values.	substring(<i>list1</i>,<i>indexPosition1</i>, <i>indexPosition2</i>) substring([\$fdGroup1:fdStr1\$], 5) substring([\$fdGroup1:fdStr1\$], 5, 10)
split	Splits <i>string1</i> into a list by <i>delimiter</i> as the delimiter. The <i>delimiter</i> is regular expression.	split(<i>string1</i>,<i>delimiter</i>) Example: split('abc2def3ghi7', '[0-9]') result is list of abc, def, ghi. Any digit from 0-9 is a delimiter.

Table 173. Examples of expressions for string operands and functions

Expression	Result	Note
'Control last updated on' + format (max ([\$Child:SoxControl/System Fields>Last Modification Date\$]))	Control last updated on October 29, 2020	Given that the object was last updated on October 29, 2020

Functions for lists and numerical values

Functions for lists and numerical values can be used in expressions.

For more information about lists and a video tutorial, see [“Working with lists”](#) on page 475.

The following functions can be used on lists and numbers, including dates and currencies.

Table 174. Functions for lists and numbers

Function	Description	Syntax
append	Result is a list, where given items are appended at the end. Requires the list and the specified items to append.	append (listName, item1, item2, ...) Examples: append ([\$Child:object type/field group:field name\$], 5, 10, 15) append([\$listOperation\$], 5, 10, 15) append([\$listOperation\$], 'test1', 'test2', 'test3') min (append ([\$objField1\$] , 0.0))
at	Result is the field value of the item at the specified index position. Count -1 returns the last item in the list.	at (listName, indexPosition) Examples: at ([\$Child:object type/field group:field name\$], 5) at ([\$objField1\$], count ([\$objField1\$]) -1)
avg	Result is a numerical average. Requires one argument, which is an object field or list. Valid for numbers, currencies, and dates.	avg (listName) Examples: avg ([\$Child:object type/field group:field name\$]) avg(5, 10, 15, 20) avg(list (5, 10, 15, 20)), builds the list and calculates the average

Table 174. Functions for lists and numbers (continued)

Function	Description	Syntax
count	Result is the number of objects or items that are counted. Requires one argument, which is an object field or list. Can optionally use Append and Remove with count.	count (listName) Examples: count ([Child:object type/ field group:field name\$]) result is the number of child objects
list	Result is a list of items. Multiple arguments allowed.	list (listName, item1, item2, ...) Examples: list ('test1','test2','test3')
max	Result is the maximum value in a list of values. Valid for numbers, currencies, and dates.	max (listName) Examples: max ([Child:object type/field group:field name\$])
min	Result is the minimum value in a list of values. Valid for numbers, currencies, and dates.	min (listName) Examples: min ([Child:object type/field group:field name\$]) min(5, 10, 15, 20) min(list(5, 10, 15, 20))
remove	Result is a list, where specified items have been removed. Provide the list and the specified items to remove. If items occur multiple times in a list, all occurrences are removed.	remove (listName, item1, item2, ...) Examples: remove(list('userA', 'userB', 'userC'), 'userB')
round	Result is to round a value. Valid for numbers. If the argument is a list of values, the result is a list of rounded values.	round (number) Examples: round ([Child:object type/ field group:field name\$])
square	Result is the square value of a single number. Valid for numbers. If the argument is a list of values, the result is a list of squared values.	square (number) Examples: square ([Child:object type/ field group:field name\$])
sum	Result is a sum of a collection of values. Valid for numbers and currencies.	sum (listName) Examples: sum ([Child:object type/field group:field name\$])

Table 175. Examples of expressions that use functions for lists		
Expression	Result	Note
count([\$Child:SOXBusEntity/ OPSS-BusEnt:Entity Type\$])	4	Given that there are 4 child objects
at ([\$Child:SOXBusEntity/ System Fields:Description\$],5)	Organizational Unit	Given that "Organizational Unit" is the description of the object in the 6th position.
min(5, 10, 15, 20)	5	
list('test1', 'test2', 'test3')	'test1','test2','test3'	Builds a list of items.
count(list ('test1', 'test2'))	2	Builds a list and counts the items in it.
count (append([\$Child:object type/field\$] , 'test3'))	Result is the number of child objects plus 1	Adds to a count.

Functions for dates

Date functions can be used in expressions.

Date functions can set an object field, be is used in an if/else statement, or be used by other functions. There are also two system variables for dates, [\$TODAY\$] and [\$DaysFromNow/\$].

The following functions can be used for dates:

Table 176. Functions for dates		
Function	Description	Syntax
add_days	Result is a date, the date given plus the number of days given. Requires two arguments. If <i>date</i> is a list of dates, the add_days function is applied to all items in the list. The result is a list of dates.	add_days(<i>date</i>,<i>number</i>) Example: add_days(2020-10-10, 2) result is 2020-10-12.
add_months	Result is a date, the date given plus the number of months given. Requires two arguments. If <i>date</i> is a list of dates, the add_months function is applied to all items in the list. The result is a list of dates.	add_months(<i>date</i>,<i>number</i>) Example: add_months(2020-10-10, 2) result is 2020-12-10.
add_year	Result is a date, the date given plus the number of years given. Requires two arguments. If <i>date</i> is a list of dates, the add_year function is applied to all items in the list. The result is a list of dates.	add_years(<i>date</i>,<i>number</i>) Example: add_years(2020-10-10, -2) result is 2018-10-10.

Table 176. Functions for dates (continued)

Function	Description	Syntax
end_of_month	Result is a date that is the last day of the month, relative to the month in the date given. Requires one argument. If <i>date</i> is a list of dates, the end_of_month function is applied to all items in the list. The result is a list of month-end dates.	end_of_month(<i>date</i>) Example: end_of_month(2020-10-10) result is 2020-10-31, if the date is in October end_of_month([D1\$]) result is 2020-10-31 if the date is in October
end_of_quarter	Result is a date that is the last day of the quarter, relative to the date given. Requires one argument. If <i>date</i> is a list of dates, the end_of_quarter function is applied to all items in the list. The result is a list of quarter-end dates.	end_of_quarter(<i>date</i>) Example: end_of_quarter(2020-10-10) result is 2020-12-31.
end_of_year	Result is date that is the last day of the year, relative to the date given. Requires one argument. If <i>date</i> is a list of dates, the end_of_year function is applied to all items in the list. The result is a list of year-end dates.	end_of_year(<i>date</i>) Example: end_of_year(2020-10-10) result is 2020-12-31.
today	Result is today's date. Requires no argument.	today() Example: [D1\$] == (today)
tomorrow	Result is tomorrow's date. Requires no argument.	tomorrow() Example: [D1\$] == (tomorrow)
yesterday	Result is yesterday's date. Requires no argument.	yesterday() Example: [D1\$] == (yesterday)

Regardless of how dates are displayed in your locale, the following expressions are valid:

Table 177. Examples of expressions that use dates

Expression	Result	Note
[TODAY\$]	2020-11-09	Given that today's date is November 9, 2020
[TODAY\$]+10	2020-11-19	Given that today's date is November 9, 2020
2020-10-10 +30	2020-11-09	
format (2020-10-10 +30)	November 9, 2020	

Table 177. Examples of expressions that use dates (continued)		
Expression	Result	Note
end_of_month(today())	2020-11-30	Given that today's date is in November 2020
format (end_of_month(today()))	November 30, 2020	Given that today's date is in November 2020
format (end_of_quarter(today()))	December 31, 2020	Given that today's date is in October, November, or December 2020

Functions for currency values

Functions for currency values can be used in expressions.

The following functions can be used for currencies:

Table 178. Functions for currencies		
Function	Description	Syntax
base_amount_of	Result is base amount value from a currency function or currency object field. If the first argument is a list of currency values, the result is a list of base amounts.	base_amount_of(currencyResult) Examples: base_amount_of (currency (1000.0 , 'EUR', 1.1)) base_amount_of([<i>\$field</i> group:field name\$])
base_code_of	Result is base currency code from a currency function or currency object field. If the first argument is a list of currency values, the result is a list of currency codes.	base_code_of(currencyResult) Example: base_code_of([<i>\$field</i> group:field name\$])
currency	Result is a representation of a currency amount, currency code, and exchange rate. If the first argument is a list of integer or decimal values, the result is a list of currency values.	currency(amount, currencyCode, exchangeRate) Examples: currency(1800000, 'JPY', 0.01)
local_amount_of	Result is local amount value from a currency function or object field. If the first argument is a list of currency values, the result is a list of local amounts.	local_amount_of(currencyResult) Example: local_amount_of([<i>\$field</i> group:field name\$])
local_code_of	Result is local currency code from a currency function or object field. If the first argument is a list of currency values, the result is a list of currency codes.	local_code_of(currencyResult) Example: local_code_of([<i>\$field</i> group:field name\$])

Table 178. Functions for currencies (continued)		
Function	Description	Syntax
ex_rate_of	Result is exchange rate from a currency function or object field.	ex_rate_of(currencyResult) Example: ex_rate_of([\$field group:field name\$])
system_ex_rate_of	Result is the system exchange rate, either current or for a specific date. Can have one or two arguments. Argument one is a currency code and two is a date. If currency code is given, result is the current system exchange rate for that currency. If two arguments are given, result is the system exchange rate for a currency code on a given date.	system_ex_rate_of(currencyCode, date) Example: system_ex_rate_of('USD', 2015-12-01) system_ex_rate_of('USD')

Examples:

Table 179. Examples of expressions that use currencies		
Expression	Result	Note
currency (1500, 'USD') + currency (150000.00, 'JPY', 0.01)	local Currency =USD exchangeRate=1.0 baseAmount=3000.0 baseCurrency=USD localAmount=3000.0	
format (currency (1500, 'USD') + currency (150000.00, 'JPY', 0.01))	USD 3,000.00	

If/then/else/endif statements

An expression can contain an if/then/else/endif statement.

Table 180. If/then/endif statements in expressions		
Function	Description	Syntax
if then elif else endif	elif is not required	if (condition) then action1 elif <...> else action N endif Example: if ([\$fdGroup1:fdName1\$] == 'enum1') then 'Medium' else 'High' endif

Table 180. If/then/endif statements in expressions (continued)

Function	Description	Syntax
Operands that can be used in conditions: == Equal != Not equal > Greater-than < Less-than >= Greater-than or equal <= Less-than or equal OR AND NOT AND NOT	Operands that can be used in conditions	Example: <pre>if ([\$abc\$] == 10 OR ([\$abc\$] == 20 AND NOT [\$def\$] == 15))</pre>
contains exists regex	Functions that can be used in conditions	Examples: <pre>exists([\$fdGroup1:fdName1\$]) contains([\$fdGroup1:string field\$], 'test') regex([\$fdGroup1:string field\$], '\d?abc.*')</pre>
in in_group matches_any in_hierarchy	Clauses that can be used in conditions	Examples: <pre>[\$fdGroup1:enum1\$] in ('aaa', 'bbb', 'ccc')</pre>

Basic example

```
if [$OPSS-Risk-Qual:Inherent Impact$] > 5 then "High Impact" else "Low Impact" endif
```

Result is High Impact, given that the value of [\$OPSS-Risk-Qual:Inherent Impact\$] is greater than 5

exists function

```
if exists([$System Fields:Name$]) then "Test BE Asia Pac" else "Not Found" endif
```

Result is: Test BE Asia Pac

contains function

```
if contains([$System Fields:Description$], 'test') then "Description has test" else "Not Found"
endif
```

Result is: Description has test

regex function

```
if regex([$System Fields:Description$], '^(?!test$).+')
then "Result: ^ start of string , ?!test$).+ the string cannot be equal to test and .+ 1 or
more characters"
else "don't match"
endif
```

The result is:

```
^ start of string , ?!test$).+ the string cannot be equal to test and
.+ 1 or more characters
```

Syntax for nested if/then/else/endif statements

The following example illustrates the syntax for a nested if/then/else/endif statement. Note that a closing else block is always needed.

```
if ( A == 123 ) then
  if ( B AND C ) then X1
  elif ( NOT B AND C ) then X2
  else X3 endif
elif ( A == 456 ) then
  if ( B AND C ) then X4
  elif ( NOT B AND NOT C ) then X5
  else X6 endif
else X7
endif
```

Example: Inherent Exposure calculation on the SOXRisk object type

```
/**
 * Risk Inherent Exposure
 * The exposure value comes from the frequency multiplied by the severity.
 * The frequency is derived from the Preference object based on the Likelihood.
 * The severity is derived from the Preference object based on the Impact.
 */
( if ([$OPSS-Risk-Qual:Inherent Likelihood$] == '1') then [$Preference/OPSS-Pref:Freq1$]
  elif ([$OPSS-Risk-Qual:Inherent Likelihood$] == '2') then [$Preference/OPSS-Pref:Freq2$]
  elif ([$OPSS-Risk-Qual:Inherent Likelihood$] == '3') then [$Preference/OPSS-Pref:Freq3$]
  elif ([$OPSS-Risk-Qual:Inherent Likelihood$] == '4') then [$Preference/OPSS-Pref:Freq4$]
  elif ([$OPSS-Risk-Qual:Inherent Likelihood$] == '5') then [$Preference/OPSS-Pref:Freq5$]
  elif ([$OPSS-Risk-Qual:Inherent Likelihood$] == '6') then [$Preference/OPSS-Pref:Freq6$]
  elif ([$OPSS-Risk-Qual:Inherent Likelihood$] == '7') then [$Preference/OPSS-Pref:Freq7$]
  elif ([$OPSS-Risk-Qual:Inherent Likelihood$] == '8') then [$Preference/OPSS-Pref:Freq8$]
  elif ([$OPSS-Risk-Qual:Inherent Likelihood$] == '9') then [$Preference/OPSS-Pref:Freq9$]
  else [$Preference/OPSS-Pref:Freq10$] endif ) *
( if ([$OPSS-Risk-Qual:Inherent Impact$] == '1') then [$Preference/OPSS-Pref:Sev1$]
  elif ([$OPSS-Risk-Qual:Inherent Impact$] == '2') then [$Preference/OPSS-Pref:Sev2$]
  elif ([$OPSS-Risk-Qual:Inherent Impact$] == '3') then [$Preference/OPSS-Pref:Sev3$]
  elif ([$OPSS-Risk-Qual:Inherent Impact$] == '4') then [$Preference/OPSS-Pref:Sev4$]
  elif ([$OPSS-Risk-Qual:Inherent Impact$] == '5') then [$Preference/OPSS-Pref:Sev5$]
  elif ([$OPSS-Risk-Qual:Inherent Impact$] == '6') then [$Preference/OPSS-Pref:Sev6$]
  elif ([$OPSS-Risk-Qual:Inherent Impact$] == '7') then [$Preference/OPSS-Pref:Sev7$]
  elif ([$OPSS-Risk-Qual:Inherent Impact$] == '8') then [$Preference/OPSS-Pref:Sev8$]
  elif ([$OPSS-Risk-Qual:Inherent Impact$] == '9') then [$Preference/OPSS-Pref:Sev9$]
  else [$Preference/OPSS-Pref:Sev10$] endif
)
```

Example: Inherent Rating calculation on the SOXRisk object type

```
/**
 * Risk Inherent Rating
 * The squared value of the likelihood and the impact is added up, then normalized from 0.0 to
 1.0.
 * Based on the value, the Rating is set from "Low" to "Very High"
 */
if ( square( [$OPSS-Risk-Qual:Inherent Likelihood$] ) + square( [$OPSS-Risk-Qual:Inherent
Impact$] ) )
  >= ( square ( [$Setting/OpenPages/Solutions/ORM/Triggers/RCSA/XMAX$] ) +
      square ( [$Setting/OpenPages/Solutions/ORM/Triggers/RCSA/YMAX$] ) ) * 0.75
  then "Very High"
  elif ( square( [$OPSS-Risk-Qual:Inherent Likelihood$] ) + square( [$OPSS-Risk-Qual:Inherent
Impact$] ) )
  >= ( square ( [$Setting/OpenPages/Solutions/ORM/Triggers/RCSA/XMAX$] ) +
      square ( [$Setting/OpenPages/Solutions/ORM/Triggers/RCSA/YMAX$] ) ) * 0.5
  then "High"
  elif ( square( [$OPSS-Risk-Qual:Inherent Likelihood$] ) + square( [$OPSS-Risk-Qual:Inherent
Impact$] ) )
  >= ( square ( [$Setting/OpenPages/Solutions/ORM/Triggers/RCSA/XMAX$] ) +
      square ( [$Setting/OpenPages/Solutions/ORM/Triggers/RCSA/YMAX$] ) ) * 0.25
  then "Medium"
  else "Low"
endif
```

Example: KRI Indicator trend calculation

```
/**
 * KRI Indicator trend
 * Calculated by comparing recent two KRI Value Bleach Status and set among Not Determined/
Steady/Worse/Better
 */
// case1 : not enough KRI values
if count( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVAL:Value
Date$] ) < 2 then "Not Determined"
// case2 : one of the recent has "Not Determined"
elif ( ( at( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-
KRIVAL:Value Date$], 0) == "Not Determined" ) OR
      ( at( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVAL:Value
Date$], 1) == "Not Determined" ) ) then "Not Determined"
// case 3 : two recent ones have the same bleach status
elif at( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVAL:Value
Date$], 0) ==
      at ( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVAL:Value
Date$], 1) then "Steady"
// case 4: The latest has "Red", which means prior one is "Yellow" or "Green"
elif at( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVAL:Value
Date$], 0) == "Red" then "Worse"
// case 5: The latest has "Green", which means prior one is "Yellow" or "Red"
elif at( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVAL:Value
Date$], 0) == "Green" then "Better"
// case 6 : The latest has "Yellow"
elif at( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVAL:Value
Date$], 1) == "Red" then "Better"
else "Worse" endif
```

Example: Audit Plan Actual T&E expenses

```
/**
 * Audit Plan actual T&E aggregation
 */
if exists( [$Child:Timesheet/System Fields:Name$] ) then
sum( [$Child:Timesheet/OPSS-Timesheet:Actual TE$] )
else 0.0 endif
```

Example: Audit Plan Actual hours

```
/**
 * Audit Plan actual hours aggregation
 */
if exists( [$Child:Timesheet/System Fields:Name$] ) then
```

```

sum( [$Child:Timesheet/OPSS-Timesheet:Monday$] ) +
sum( [$Child:Timesheet/OPSS-Timesheet:Tuesday$] ) +
sum( [$Child:Timesheet/OPSS-Timesheet:Wednesday$] ) +
sum( [$Child:Timesheet/OPSS-Timesheet:Thursday$] ) +
sum( [$Child:Timesheet/OPSS-Timesheet:Friday$] ) +
sum( [$Child:Timesheet/OPSS-Timesheet:Saturday$] ) +
sum( [$Child:Timesheet/OPSS-Timesheet:Sunday$] )
else 0.0 endif

```

Example: Audit Plan Helper

```

/**
 * URL for audit plan Helper
 */
[$APPLICATION_URL$] + "/Wizard/OPS_AuditAddModifyPlans.jsp?resourceId=" + [$System
Fields:Resource ID$] +

"<a style='color:#003F87' href='/Wizard/OPS_AuditAddModifyPlans.jsp?resourceId=" +
[$System Fields:Resource ID$] +
">" +
[$System Fields:Name$] +
"</a>"

```

Running a calculation as an administrator

An administrator can run a calculation for multiple objects at once.

Before you begin

The calculation must be defined, enabled, and published. For more information, see [“Defining a calculation”](#) on page 467.

Optionally, customize the content of email notifications. For more information, see [“Customizing email notifications for GRC Calculations”](#) on page 492.

About this task

When an administrator runs a calculation, it runs for all objects that meet both the conditions that are defined in the calculation's applicability and conditions that are defined on the input fields.

You can run a single calculation at a time. It is not possible to start multiple calculations at once.

Procedure

1. Click  > **Solution Configuration** > **Calculations**.
2. Select the check box next to a single calculation and click .

An estimated number of affected objects is displayed. The number reflects all objects that match the criteria that is defined in the calculation's applicability.
3. Click **Start Calculations** to continue.
4. Click Done.

Results

The calculation starts.

Track the progress and results by monitoring the following columns on the Calculation List:

- **In Queue**

Displays the total number of objects that are still to be processed.

- **Next In Queue**

Displays the next five objects in the queue to be processed. Click an object to open it in a Task View.

- **Error Count**

Displays the total number of objects that encountered an error.

Refresh the screen to display the latest information as the calculation progresses.

After the calculation finishes, an email is sent to the administrator who started the job.

What to do next

Review the email that you received as the administrator who started the calculation.

Check the results:

- Verify that the correct objects were updated.
- Verify that the calculation result is correct.

If the calculation failed for any objects, investigate the cause. For more information, see [“Testing and debugging a calculation”](#) on page 491.

Testing and debugging a calculation

Verify the results of a calculation and resolve errors that are encountered.

There are several areas to review when testing and debugging a calculation:

- Accuracy

Does the calculation run without errors and update the correct fields?

Are the values in the updated fields correct?

- Interaction in a Task View

Is the user interaction in a Task View working as you expect?

- Applicability

Are the correct objects subject to the calculation?

- Conditions on the input field

Are the correct objects subject to the calculation?

- Errors

What error messages are issued? How can you use them to guide you to a resolution?

In the Task Focused UI, errors for the current session display as notifications.

Accuracy

Test the calculation by running it as an administrator.

If you run a calculation as an administrator, there are several ways you can watch for problems:

- Monitor the **In Queue**, **Next in Queue**, and **Error Count** columns in the Calculation List. Refresh the screen to display the latest information as the calculation progresses.
- Review the email that you received as the administrator who ran the calculation. The email lists all the objects that failed. Open those objects and review the error messages that are saved on the objects themselves.

Note: It is helpful when debugging a calculation to define a Grid View that contains the fields that a calculation should set. Run the calculation as an administrator and use the Grid View to quickly verify that the fields are set with the correct values. Continue to modify, run, and verify the results in the Grid View until the calculation is fully tested. Refresh the screen to display the latest information in the Grid View.

Interaction in a Creation View and a Task View

Test the calculation by creating an object with a Creation View. Then, test it in a Task View that users work with. When users are working on a Task View and add or change the value of a field that is an input field for a calculation, the calculation runs and the set fields are updated. If an error is encountered, an error message displays as the user is working. Verify the contents of the Task View and that the correct fields display. Be prepared to support users when they encounter errors and resolve the problems.

Applicability

Test that the correct objects are subject to the calculation. Review how the Applicability is defined on the calculation and test it thoroughly.

Conditions on input fields

Test that the correct objects are subject to the calculation. Review how conditions are defined on input fields in the calculation and test them thoroughly.

Error messages

When a calculation encounters a problem, an error message is saved on the object. The error message is cleared in the Task Focused UI after the problem is resolved.

Error messages are assigned a unique ID so that you can match what happened in the UI with the stack trace in the aurora log file. For example, if the system issues an error, UJA0J1RX75PA-OP-11604, search for UJA0J1RX75PA in the log file. The descriptive text, can also guide you to a solution.

When a calculation encounters a problem, an error message is saved on the object. The error message is cleared in the Task Focused UI after the problem is resolved.

If you get an error message `Insufficient information`, check that the calculation contains an `if exist/then/else` statement. This error can occur if the statement has no `else` statement, meaning that there is no default if none of the conditions are met.

Customizing email notifications for GRC Calculations

You can customize the content of the email notifications that are generated by GRC Calculations by defining application text that is specific to your organization.

Before you begin

Learn about starting calculations in bulk as an administrator. For information, see [“Running a calculation as an administrator”](#) on page 490.

About this task

At the end of a bulk update process, an email notification is sent to the administrator who started the process.

You can use the default email template as-is or customize the text to meet your requirements. There is one email template for all calculations and all object types. You cannot create a new template.

If you operate in multiple locales, you can define email content in different languages. The template is designed for multiple formats, including tablets and phones.

If you customize the text, you define the content of the email notifications by using application text strings. The email subject content is plain text. The email body content is formatted in HTML. You can apply styles using embedded stylesheets.

You can also insert variables and fields in the email body content. The following variables are applicable to calculations:

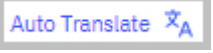
- [{\$CALC_NAME\$}] - calculation name
- [{\$OBJECT_COUNT\$}] - number of objects processed
- [{\$SUCCESSFUL_CALCULATION_COUNT\$}] - number of objects processed successfully
- [{\$DISPLAY_FAILURE\$}] - includes failure information, if existent
- [{\$FAILED_CALCULATION_COUNT\$}] - number of objects that failed
- [{\$FAILURES\$}] - list of failures

Example:

```
<html>
  <head></head>
  <body style="font-family: ibm-plex-sans,HelveticaNeue,Helvetica,Arial,sans-serif; font-size: 14px;">
    <h1 style="font-size: 20px; font-weight: 300; padding: 22px 24px;">IBM <span style="font-weight: 600">OpenPages with Watson</span></h1>
    <hr style="margin: 0; border-bottom: 2px solid #0f62fe" />
    <div style="padding: 8px 24px 32px; background-color: #f3f3f3;">
      <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">Calculation
name:</h2>
      <p style="margin: 0">[{$CALC_NAME$}]</p>
      <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">Object type:</h2>
      <p style="margin: 0">[{$System Fields:Object Type Label$}]</p> </div>
    <div style="padding: 8px 24px 160px;">
      <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;"> Number of objects
evaluated:</h2>
      <p style="margin: 0">[{$OBJECT_COUNT$}]</p>
      <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;"> Number of
calculations run successfully:</h2>
      <p style="margin: 0">[{$SUCCESSFUL_CALCULATION_COUNT$}]</p>
      <div style="display: [{$DISPLAY_FAILURE$}]">
        <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;"> Number of
calculations failed to run:</h2>
        <p style="margin: 0">[{$FAILED_CALCULATION_COUNT$}]</p>
        <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;"> Failed
calculations (first 100 objects):</h2>
        <ul> [{$FAILURES$}] </ul> </div> </div>
      <hr style="margin: 0; border-bottom: 1px solid #767676" />
      <div style="padding: 32px 24px;">This email was automatically generated by
[{$ApplicationText/product.name$}].</div>
    </body>
  </html>
```

Procedure

1. Click  > **System Configuration** > **Application Text**.
2. Click  to access the search filter.
3. Click **Email Templates**.
4. Open the **Email Templates** folder.
5. Use **Search** to further refine the list.
6. Select the application text you want to modify:
 - com.calculation.email.template.bulk.run.subject contains the text in the subject line.
 - com.calculation.email.template.bulk.run.body contains the text in the body of email.
 - com.calculation.email.template.bulk.run.failure.part contains a URL to the Task View that opens when an object in a list is clicked.
7. For each locale, enter the content that you want to appear in the email notification.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

8. Click **Done**.

Chapter 15. Configuring GRC Workflow

Using the GRC Workflow feature, you can design, configure, and administrate workflow definitions and workflow instances for OpenPages.

Setting up GRC Workflow

You must configure workflows before users can access and use them.

Before you begin

Complete the following prerequisites:

- Learn about the GRC Workflow feature in OpenPages. For information, see [“GRC Workflow fundamentals”](#) on page 496.
- Learn about what you need to consider when you design a workflow. For information, see [“Designing a workflow”](#) on page 505
- Learn about oversight users and the Oversight Tasks tab. For more information, see [“Types of users who interact with workflows ”](#) on page 498 and the *IBM OpenPages with Watson User Guide*.
- Configure the Task Focused UI before you configure the GRC Workflow feature with the exception of Task Views, which can be designed concurrently with GRC Workflow. For information, see [“Setting up the Task Focused UI”](#) on page 363.
- Learn about GRC Calculations. For information, see [Chapter 14, “Configuring GRC Calculations,”](#) on page 457.
- Learn about the Scheduler. For information, see [Chapter 16, “Scheduler,”](#) on page 551.

About this task

During the configuration process, complete the following tasks to prepare for implementing workflows in OpenPages.

Procedure

1. Review your current implementation of triggers and configurable lifecycles and make changes accordingly.

When your organization adopts GRC Workflow, you do not have to retire the triggers and configurable lifecycles to use workflows. You can design a landscape that uses all three features, but be aware of the limitations.

- You can use both triggers and workflows on the same object type but you must disable triggers that overlap with functionality in workflows. You can add custom actions to the workflows to accomplish what is currently achieved by triggers.
- You can use both configurable lifecycles and workflows for the same object type, but consider how they interact and where they conflict. For each object type, you can continue using configurable lifecycles or move what you currently accomplish with configurable lifecycles to workflows. If an object type has both a workflow and a configurable lifecycle, the workflow **Actions** button in Task Views in the Task Focused UI takes priority over the lifecycle **Actions** button. Lifecycle fields that are used by configurable lifecycles are redundant in workflows. To disable lifecycles, remove the XML from the registry settings for lifecycles. For information, see *Configuring Triggers* in the *IBM OpenPages with Watson Trigger Developer Guide*.
- Determine how you use the Standard UI and the Task Focused UI. Workflows are available only in the Task Focused UI. You might choose to continue using configurable lifecycles in the Standard UI

- for some object types and use workflows in the Task Focused UI for other object types. You can also choose to use configurable lifecycles in both UIs.
2. Update the permissions for role templates for administrators who are configuring the workflows.
 - a) Click **Administration > Role Templates > <role template> > Role Permissions**.
 - b) Select the **SOX > Administration > Workflow** permission.

Administrators with this permission enabled can define workflows with  > **System Configuration > Workflows**. They can also access and terminate workflow instances from **Manage Workflows**. For more information, see [“Managing workflow instances”](#) on page 547.
 3. Define the sender email address that is used for email notifications. It is defined in the **Solutions > ORM > Email > From Email** registry setting.
 4. Define the maximum number of recipients for emails. It is defined in the **Platform > Workflow Implementations > OpenPages > Maximum Recipients Per Email** registry setting.
 5. Define whether workflow information card content is updated automatically when changes are made to an object. It is defined in the **Platform > Calculation > Refresh Workflow Information Automatically** registry setting. If set to true, **Platform > Calculation > Enabled** must also be set to true. For more information, see [“How users interact with workflows”](#) on page 499.
 6. Optional: Customize the content of the email notifications. Assignees and subscribers can receive email notifications for each action in a workflow. You can use the default email template or customize the text to meet your requirements. For information, see [“Customizing email notifications for GRC Workflow”](#) on page 548.
 7. Review your implementation of Task Views in the Task Focused UI or design them concurrently as you configure GRC Workflow. Learn about Task Views if you are not familiar with how to define and use them. For information, see [“Planning the Task Views”](#) on page 380.
 8. Define, test, and implement workflows. For information, see [“Defining a workflow”](#) on page 513.

What to do next

Complete the following post-requisites:

- Export workflow definitions from one environment to another, as needed. For information, see [“Exporting and importing workflow definitions”](#) on page 548.
- Monitor workflow instances. For information, see [“Managing workflow instances”](#) on page 547.
- Start workflow instances in bulk, as needed. For information, see [“Starting workflow instances in bulk”](#) on page 546.
- Report authors can include information from workflow instances in reports. For information, see [“Reporting on information in workflow instances”](#) on page 550.

GRC Workflow fundamentals

OpenPages provides the framework that you use to define workflows and build task views that users access to start and interact with workflow instances.

Show me how

This video provides an overview of GRC Workflow and the Workflow Designer.

<https://youtu.be/ap5ulBKetIE>

Workflow definitions and workflow instances

The OpenPages GRC Workflow feature is based on workflow definitions and workflow instances.

You define workflows using the GRC Workflow Designer, which is a graphical editor in the Task Focused UI. After you publish a workflow, it is available in OpenPages.

Workflow definitions

A workflow definition represents a business process and describes the tasks involved in the process. A workflow is defined for one object type. An object type can have multiple workflow definitions, for example, for Controls, you might have two workflows: Control Assessment and Control Change Request. The two workflows reflect two different business processes for Controls. Although an object type can have multiple workflow definitions, an object can be involved in only one workflow at a time. For example, if Control ABC is going through the Control Assessment workflow, you cannot start the Control Change Request workflow for it.

A workflow definition has the following characteristics:

- A workflow definition is static.

The actual execution of the workflow is described by the workflow instance, which holds the run-time information.

- A workflow definition is versioned.

Each time a workflow definition is published, a new version of that workflow definition is made available to users. The new version is used for workflow instances that are started after it is published. It does not affect workflow instances that are already running.

- A workflow definition can be disabled.

When a workflow definition is disabled, no new workflow instances based on that workflow definition can be started. Workflow instances that were already running when the workflow definition was disabled continue to run. Disabled workflow definitions can be re-enabled.

A workflow definition is made up of the following elements:

- Workflow properties define basic information about the workflow.

You can define how the workflow can be started (manually or automatically), a start schedule, the oversight user, the overall due date, applicability, and criticality normalization. For more information, see [“Defining workflow properties”](#) on page 514.

- Stages represent tasks that are assigned to users.

There are three types of stages: start, end, and standard. For information, see [“Workflow stages”](#) on page 519.

- Actions control the transitions between stages and the values on the **Actions** button.

An action contains comment settings, conditions, validations and operations, email notification settings, and a setting that controls whether the action runs in the background. For information, see [“Defining a workflow action”](#) on page 527.

Workflow instances

As users work in OpenPages, they launch instances of workflow definitions. A workflow definition can have an unlimited number of workflow instances in progress at any given time.

Administrators can view and terminate active workflow instances. For more information, see [“Managing workflow instances”](#) on page 547.

How workflows are started

The workflow properties defined how a workflow can start.

A workflow can be started in the following ways:

- Automatically when an object of the object type is created (if **Type** in the workflow properties is set to Auto Start).
- Manually when a user accesses the object and clicks an option on the **Actions** button (if **Type** in the workflow properties is set to Manual Start).

- Automatically at set times (if **Scheduled Start** in the workflow properties is defined).

Workflows that are defined with a **Scheduled Start** automatically display as jobs in the Scheduler.

- By an administrator who clicks the **Start Job** option in the Scheduler (if the workflow is defined with a **Scheduled Start** in the workflow properties). For more information, see [“Managing jobs ” on page 551](#)
- By an administrator who clicks the **Start Workflow** option on the Workflow List. For more information, see [“Starting workflow instances in bulk” on page 546](#).

After a workflow has started, other workflows start in the following ways:

- An action on a workflow can start another workflow for a related object.
- When a workflow ends, another workflow for the same object can start.

A workflow can have **Type** set to Auto Start or Manual Start and also be defined with a scheduled start. The type and scheduled start are independent of each other. If a workflow is set to Auto Start, a scheduled start can be used to restart a workflow that has already completed.

For all start methods, a workflow starts only if the **Applicability** conditions in the workflow properties are met.

You can use **Applicability** conditions to restrict when a workflow starts, for example, you can restrict who can start the workflow to a specific user or user group. Without these conditions, any user can start a workflow.

For a workflow that is defined to start on a schedule, you can, for example, use **Applicability** conditions to start a workflow only if a Review Date is equal to today's date. Another option is to start a workflow in advance of a due date, relative to today's date. For example, a workflow for Control objects should start 6 weeks before the next assessment is due, giving the team enough time to complete the assessment. In this case, add an **Applicability** condition based on the due date field, set Expression to [\$TODAY\$], set **Adjust Date By** to A specified value, and enter 42 in **Number of Days**.

For more information about **Type** and **Applicability**, see [“Defining workflow properties ” on page 514](#).

Types of users who interact with workflows

Three types of users interact with workflows: assignees, subscribers, and oversight users.

• Assignees

Assignees are users who own a task in a workflow. Assignees are defined per stage. There can be many assignees at a time for a task and different ones throughout a workflow process. Assignees view and find their assignments on the dashboard and My Tasks tab. If the assignee for a stage is a user group, the task is displayed on the dashboard or My Tasks tab for all users in the group. Any user in the group can pick up the task and complete it. Depending on how the workflow is configured, assignees can receive email notifications each time the stage changes and when a workflow ends. Assignees can also receive email reminders before, on, and after a stage due date.

• Subscribers

Subscribers are users who have an interest in one or more stages of a workflow. For example, the owner of the parent object in a workflow can be designated as a subscriber. Subscribers are frequently set to fields on the related object. They do not own tasks but they can complete tasks, if they choose to. They can act as a backup for the assignees. Subscribers are defined per stage. There can be many subscribers at a time for a task and different ones throughout a workflow process. Subscribers can view work that they are subscribed to on the Subscription Tasks tab. Depending on how the workflow is configured, subscribers can receive email notifications each time the stage changes and when a workflow ends. Subscribers can also receive email reminders before, on, and after a stage due date.

• Oversight users

An oversight user is someone who has overall responsibility for an area. Oversight users are defined per workflow. There can be none, one, or many oversight users for a workflow instance. Oversight users are ordinarily at a management level, for example, Division Leads. In a situation where there are

multiple divisions, each Division Lead can track workload and tasks for their teams. At any time during a workflow, they can add information to a task or complete it, if they choose to. Depending on how the workflow is configured, oversight users receive email notifications when a workflow ends. Otherwise, they do not receive email notifications. They access the Oversight Tasks tab, which summarizes tasks generated for workflows for their area. The Oversight Tasks tab summarizes tasks for assignees under one oversight user. Oversight users can drill down to the workload for specific individuals. Oversight users do not normally approve work or get assigned tasks unless a stage in the workflow also makes them an assignee or subscriber. In this case, they can access the dashboard or the My Tasks tab to view work that is assigned to them. They can access the Subscription Tasks tab to view what they are subscribed to.

See the *IBM OpenPages with Watson User Guide* for more information about the dashboard, My Tasks tab, Oversight Tasks tab, and Subscription Tasks tab.

How users interact with workflows

You can control aspects of the interaction between users and workflows. Your goal as a workflow designer is to create workflows that not only accurately model the business process but are also easy for users to finish and interact with.

As users work on their daily tasks, for example, approving or rejecting tasks that are assigned to them, workflows are behind the scenes orchestrating what happens next and who is involved. Users do not need a detailed understanding of the underlying workflow definitions or workflow instances. They simply work on their tasks until they are complete. Messages and on-screen information guide them through the process. They likely know only their part of the process and might not have a complete understanding of the full business process.

Starting a workflow

How a workflow can be started is defined in the workflow properties. For more information, see [“How workflows are started” on page 497](#).

After a workflow starts, a workflow instance is created.

Stages become tasks

A stage in a workflow definition represents a task. Every time the stage changes, a new task is created.

Stages determine participants

A stage in a workflow definition determines the participants in the task, meaning the assignees and the subscribers.

Assignees access their tasks on the dashboard and My Tasks tab

Assignees access the dashboard and My Tasks tab to find their tasks. The dashboard can be configured but My Tasks tab requires no configuration.

Subscribers access their tasks on the Subscription Tasks tab

Subscribers access the Subscription Tasks tab to find tasks that they are subscribed to. The Subscription Tasks tab requires no configuration.

Assignees and subscribers access their tasks from emails

Assignees and subscribers can receive two types of emails:

- Email notifications
- Email reminders

Email notifications can be sent every time the stage changes and when a workflow ends. The recipient of the email can click a URL in the email to access the task. Emails notifications are defined on end stages and actions between stages. The content of the email notification can be used as-is or modified to meet your requirements. Email notifications are sent as single emails, which means that a user might receive multiple per day.

Email reminders can be sent before, on, and after a stage due date. The recipient of the email can click a URL in the email to access the task. Emails reminders are defined on standard stages. You can define who receives email reminders (assignees or subscribers). The content of the email notification cannot be modified. Email reminders are sent as a summary email, which means that a user receives one email per day regardless of the number of tasks that generated a reminder.

Oversight users access the Oversight Tasks tab

Oversight users access the Oversight Tasks tab to have a summary of the workload in their area of responsibility. Oversight users are defined in the overall workflow properties, not per stage. The Oversight Tasks tab lists all open tasks that belong to workflows that the oversight user is responsible for. The Oversight Tasks tab requires no configuration.

Users can access bulk workflow actions

If the bulk workflow actions feature in GRC Workflow is used, user can access their tasks by using the **Complete task with bulk workflow actions** window. If a user has open tasks, the window is displayed on the My Tasks tab and dashboard panel, the Subscription Tasks tab and dashboard panel, and the Oversight Task tab and dashboard panel.

Assignees interact with a Task View

A stage in a workflow definition determines the Task View that an assignee opens when they access the task. The Task View must contain the appropriate fields for that stage and what the user needs to accomplish. For example, if the assignee needs to set a date field at the stage, the field must be visible and editable. Two elements on a Task View help assignee understand what to do:

- User guidance

User guidance is customer-specific help text and field information that is displayed in the right panel. You define user guidance in the Task View. If a task is part of a workflow that has started, users can click **Select an action to validate** to check whether an action would pass validation before they complete the action. Per stage you can override the Task View's user guidance text with text that is specific to that stage. Use this powerful feature to provide instructions and information that are specific to your organization and your business processes.

- Workflow information card

Workflow information is displayed in the right panel of any object that is in a workflow process. Called the *workflow information card*, this panel displays the stage that the object is currently at, the stage due date, and the current assignee. It is displayed regardless of who opens the object. You do not have to modify the task views to make it display.

Whether the workflow information card is automatically updated when an object is changed depends on the registry setting, **Platform > Calculation > Refresh Workflow Information Automatically**. If set to true, the content of the workflow information card is automatically updated and email notifications are sent if there is a change to assignees, subscribers, or oversight users. If set to false, the user must manually refresh the workflow information card.

Click the refresh button in the workflow information card if the workflow fields are not automatically updated with the latest changes. Fields that are displayed in the workflow information card are refreshed. If the dashboard or task tabs are open, information there is refreshed as well.

After a workflow is finished, the workflow information panel is no longer displayed.

Options on the Actions button drive the workflow

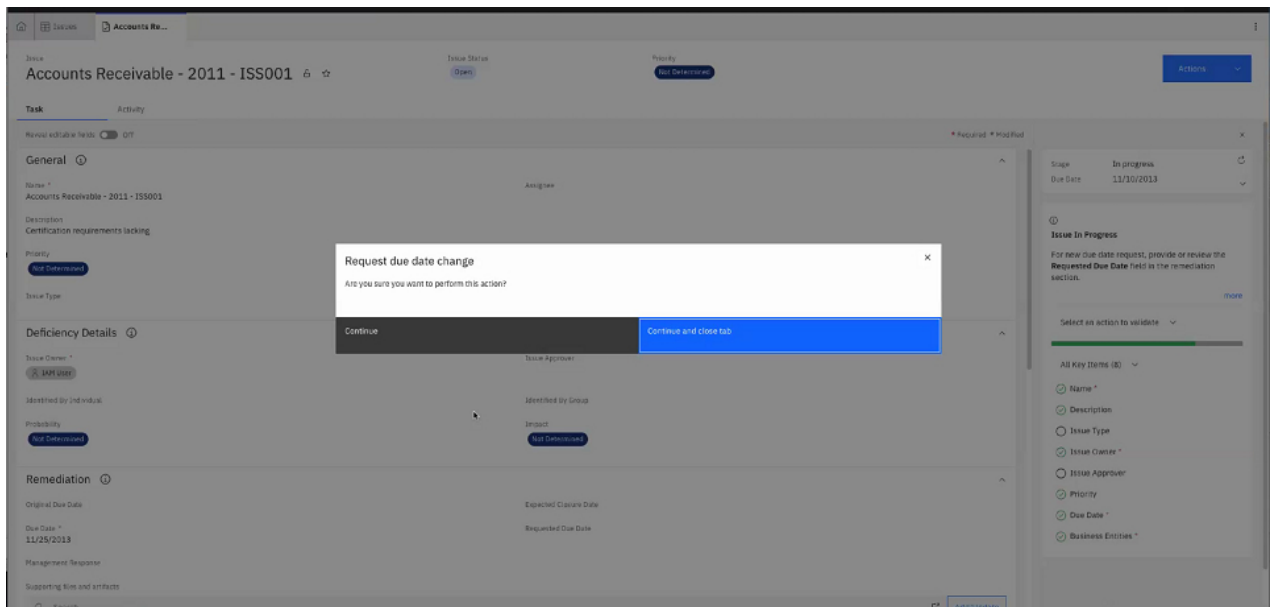
Assignees use the options on the **Actions** button to start workflows and complete their work and drive the workflow forward. You define the values that are displayed to users when you define actions between stages. The names should be short, active, and meaningful to the assignees.

If a user does not have permission to start the workflow or take the current action, no options are displayed on the **Actions** button. You can add an explanation to the user guidance to cover this situation.

Confirm the selected action

When a user chooses an action, a confirmation window is displayed. The access point determines the content of the confirmation window.

From a Task View, the confirmation window contains default content, as shown in this example:



The text on this confirmation can be customized by providing text on a workflow action in **Override workflow action text**. The text in **Override workflow action text** overrides the default text.

From a bulk workflow actions Grid View, the confirmation window contains more information, as shown in the following example:

Bulk Workflow Action (27) Unsaved Filter X Workflow Name: RCSA Stage (Status): In Review

Select the tasks you'd like to perform bulk action.

27 items selected

Name	Description
Risk Assessment 4	Risk
Risk Assessment 6	Risk
Risk Assessment 8	Risk
Risk Assessment 9	Risk
Risk Assessment 10	Risk
Risk Assessment 14	Risk
Risk Assessment 16	Risk
Risk Assessment 18	Risk
Risk Assessment 19	Risk
Risk Assessment 20	Risk

Reject X

Please review the workflow stage change. Once updating process starts, there is no undo. If you are sure you want to proceed, click Confirm. Once the process completes we'll notify you result via email and notification.

Selected Tasks: 53

Current Stage	New Stage
In Review	Closed

Workflow Action

Please enter your rejection reason below.

Rejection Comment *

Cancel Confirm

Two texts of this confirmation window can be customized:

- You can add text at the position encircled in red by defining text on a workflow action in **Override workflow action text**.
- You can define text in the `app.taskView.confirmation.action.message` application text to control the text at the top.

Users can enter comments

Users can enter a comment (reason) that can be up to 4000 characters. Whether the comment window is displayed and whether it is required or optional is defined by the workflow action. For example, for an approval stage, you can define the workflow actions so that a user must provide a comment (reason) if the REJECT action is selected but a comment is optional if the APPROVE action is selected.

Focus on due dates

The due date for a task and the overall due date for a workflow are important to the participants in a workflow. For more information, see [“Interpreting and viewing due dates” on page 505](#).

System workflow fields

Information in a workflow instance is stored in system workflow fields.

You can include system workflow fields in Task Views, insert them in the email template, and include them in reports. When you define a workflow, you can reference system workflow fields in applicability, conditions, validations, user assignments, and Filter By criteria where you can choose a field in the current object or in a related object. For example, you can reference a system workflow field in the current object or a related object in workflow Applicability conditions and in workflow action conditions and validations.

The following fields are system workflow fields:

- System Workflow Fields:Action Comment
- System Workflow Fields:Action Comment Date
- System Workflow Fields:Action Comment Owner (users or user groups)
- System Workflow Fields:Action Name (action label based on user's locale)
- System Workflow Fields:Action System Name (internal action name)
- System Workflow Fields:Assignees (users or user groups)
- System Workflow Fields>Last Action User (users)
- System Workflow Fields:Overseers (oversight users or user groups)
- System Workflow Fields:Performed Action (last performed action)
- System Workflow Fields:Stage Due Date
- System Workflow Fields:Stage Instance State (open, complete, or cancelled)
- System Workflow Fields:Stage Name (stage label based on user's locale)
- System Workflow Fields:Stage Start Date
- System Workflow Fields:Stage System Name (internal name)
- System Workflow Fields:Subscribers (users or user groups)
- System Workflow Fields:Workflow Criticality
- System Workflow Fields:Workflow Due Date
- System Workflow Fields:Workflow Name (workflow label based on user's locale)
- System Workflow Fields:Workflow Start Date
- System Workflow Fields:Workflow Start User (user) (for workflows that automatically start, this is the user who created the new object)
- System Workflow Fields:Workflow State (open, complete, cancelled, or executing)
- System Workflow Fields:Workflow Status (the label based on the user's locale of the Status field on actions)
- System Workflow Fields:Workflow Status System Name (the system name of the Status field on actions)
- System Workflow Fields:Workflow System Name (internal workflow name)

Using variables, functions, and fields

You can insert variables, object fields, system workflow fields, URLs, and application text in email templates and use them in the **expression** field. The **expression** field is part of **Applicability** in workflow properties and **Conditions**, **Validations**, and **Operations** in an action.

Variables

Table 181. Variables	
Enter	To insert/use
[\$APPLICATION_URL\$]	URL for OpenPages
[\$COGNOS_URL\$]	URL for Cognos Analytics
[\$END_USER\$]	End user identifier
[\$TODAY\$]	Today's date
[\$WORKFLOW_ACTION_USER\$]	User who completed the current action. It is used in the email template to show the user who sent an email notification.

Table 181. Variables (continued)	
Enter	To insert/use
[\$RULE_ASSIGNEES\$]	Users or groups assigned to the rule. It is used in automated workflows. The users or groups that are assigned to the rule are passed to the automated workflow.
[\$RULE_CRITICALITY\$]	Criticality of the rule. It is used in automated workflows. The Criticality of the rule is passed to the automated workflow. Valid values are: low, medium, high, or critical. Values are case sensitive.

Functions

Table 182. Functions	
Enter	To
trim	Use the trim function to reduce the length of a string field. For example, apply in an Object Name field to ensure that the value does not exceed a set limit. Syntax: <i>[\$field group:field name trim(length, replacementChar)\$]</i> Function name is case insensitive. Replacement character is optional. Examples: [\$RCM-TRRI-RegEv:Title trim(200,...)\$] Trims to first 200 characters of the field, replaces remaining additional characters with '...'. [\$RCM-TRRI-RegEv:Title trim(200,)\$] Trims to first 200 characters of the field.

Fields, URLs, and application text

Table 183. Fields, URLs, and application text	
To insert/use	Use the format
Object fields	<i>[\$field group:field name\$]</i>
System fields	<i>[\$System Fields:field name\$]</i>
A URL to an object task view	<i>[\$System Fields:Task View URL\$]</i>
Workflow field	<i>[\$System Workflow Fields:field name\$]</i> For example: <i>[\$System Workflow Fields:Action Label\$]</i>
Parent, child, preference field	<i>[\$Parent:object type/field group:field name\$]</i> <i>[\$Child:object type/field group:field name\$]</i> <i>[\$Preference/field group:field name\$]</i>

Table 183. Fields, URLs, and application text (continued)

To insert/use	Use the format
Application text content	[\$ApplicationText/ <i>application text key</i>]
Object type name	[\$System Fields: <i>Object Type Label</i>]
Registry setting value	[\$Setting/OpenPages/....\$]
Day count from today to the stage due date	[\$DaysFromNow/System Workflow Fields:Stage Due Date\$]

Interpreting and viewing due dates

The different due dates involved in workflows assist users in completing their work on time.

Workflow due date and stage due dates

A workflow instance has an overall due date and each stage has a due date. The overall due date is displayed on the Oversight Tasks tab. The stage due dates are displayed on the workflow information card and on the users' dashboards. You can also add stage due dates and overall due dates to Task Views and Grid Views. A stage due date is based on the stage entry date (the date that the workflow instance enters the stage). If a workflow instance goes back to a stage, for example, it is rejected, the stage entry date is updated to today, and the due date is recalculated. All due dates are independent of each other. Due dates are calculated as calendar days, regardless of whether they are working or non-working days.

Object due date and assignee

Workflows have a due date field and an assignee field. However, an object can also have a due date field and an assignee field. The fields are unrelated. To avoid confusion, you might want to remove the object due date and object assignee fields from the views. You can also, optionally, copy the values from the workflow due date and assignee field to the object due date and assignee fields.

Designing a workflow

Designing a workflow involves knowing your business, understanding the workflow process, planning the workflow, planning the workflow participants, and designing the task views.

Know your business

Before you design a workflow, study the business process that the workflow is modeled on. Make sure you understand every step in the process and what each person or department must accomplish. Ensure that you have a clear grasp of the business process before you get started. Make sure you also know who needs to approve your design and how the approval process works. You will want to share your design with the stakeholders and make revisions based on their input.

Plan the workflow process

After you understand the business process, plan the design of the workflow. You likely have several ways you can approach it. Look at the pros and cons of each approach before you proceed.

- What is the driver for the workflow? Do you need multiple workflows or can you use one workflow and apply conditions on **Applicability** in the workflow properties? For example, is there a different workflow based on values in the object?
- How large is the workflow? You can break a large workflow into multiple smaller workflows. To link workflows together, you define actions that start workflows for related objects and end stages that start workflows for the same object. Add validation to make the workflows dependent on each other based on specific circumstances or results.

Take care that you do not create a situation where workflows go into an infinite loop and overload the system. For example, you can inadvertently create a cascading effect when one workflow starts 1000 workflows, each of those 1000 workflows start another 1000 workflow, and so on. Safeguards are in place to avoid such a problem but they do not cover all possibilities.

- Does the workflow start automatically or manually?
- Does the workflow start on a set schedule?
- How many stages are there? Each stage creates a task.
- What needs to happen each time the stage changes? What validations need to occur at every stage change? What operations need to happen? Do fields need to be set or values calculated?
- What stages in the workflow do you want to allow users to complete as bulk workflow actions? For these stages, users can access tasks from the **Complete task with bulk workflow actions** window. It allows users to more quickly and efficiently work through the tasks they must complete.
- What are the options on the **Actions** button? What conditions must be met for an option to display? If options on the **Actions** button are displayed only to specific users, add text to the user guidance so that other users understand why no options are visible to them.
- Can a user provide a comment when they complete an action? If so, is the comment optional or required? For example, the rejection action on an approval stage can be defined to require the user to enter a comment. You can configure comments for all actions in a workflow except the initial action, which is from the start stage to the first standard stage. Plan how you want to use comment information and make it visible to other users. The workflow system fields for comment text, comment owner, and comment date can be included in task views and email notifications.
- Plan how often users receive email notifications in the workflow. Email notifications can be sent every time the stage changes and when a workflow ends. Plan the email notifications so that users are informed but not overloaded with emails.
- Plan when users receive email reminders. Emails reminders can be sent on a repeating schedule relative to a stage's due date. Plan the email reminders so that they effectively help users get their work done. Email reminders are sent as a summary email, which means that a user receives one email per day regardless of the number of tasks that generated a reminder.
- Are there points in the workflow when another workflow for a related object needs to start?
- Are there points in the workflow when child objects need to be created?
- Are there any points in the workflow when a calculation needs to be run?
- What are the cancellation or rejection paths in the workflow? At what point can a user cancel a task and what stage does the cancellation take them back to? What fields that were set by a field now need to be cleared? If an assignee must go back, how much work do they have to repeat? Plan paths in the workflow in both a forward and backward direction, as your business process requires.
- How many ways can the workflow end? You can define multiple end stages if a workflow can end in different scenarios. For example, you might have a workflow that can end in one of three ways.
 - End stage A: the workflow finishes successfully and fields 1, 2, and 3 on an object are set to the values A, B, and C.
 - End stage B: the workflow finishes successfully and fields 1, 5, and 6 on an object are set to values B, Z, and Y.
 - End stage C: the workflow is canceled and no actions are taken.
- Who needs to receive an email notification when a workflow ends? The oversight user and any other users you designate can receive an email notification when a workflow ends.
- Is the object finished when the workflow ends or does another workflow for the object need to start?
- What workflow information needs to be retained after the workflow finishes? After a workflow is finished, the workflow information on an object is no longer displayed. You need to save workflow information to objects to retain workflow information, for example, the completion date and the assignees.

Review the object structure

Understand the object structure. A workflow action that creates an object can create only a direct child object. But applicability in the workflow properties and conditions and validations on actions and the end stage can be based on field values on a related object that is a direct child, direct parent, ancestor, or descendant object.

Plan the workflow participants

After you plan the design of the workflow, map out who the workflow participants are.

- Who can start the workflow? You can restrict it by applying conditions on **Applicability** in the workflow properties.

The user who starts a workflow is saved in System Workflow Fields:Workflow Start User. Conditions where you can select **A field in the current object** or **A field in a related object** can be based on the value in this field.

- Who is the oversight user for the workflow? The oversight user is defined in the workflow properties.
- Who are the assignees for each stage? Assignees are defined by stage. The assignee gets a new task every time the stage changes. If the assignee for a stage is a user group, the task is displayed on the dashboard and My Tasks tab for all users in the group. Any user in the group can pick up the task and complete it.

The user who performed the most recently completed action is saved in System Workflow Fields:Last Action User. Conditions where you can select **A field in the current object** or **A field in a related object** can be based on the value in this field.

- Who are the participants for each stage? Participants are defined by stage.
- Who else has access to each stage of the workflow? Should users who are not workflow participants be allowed to see objects? You define access by setting the Access Type field on the stage properties.

Plan the Task Views

Workflows and task views work hand-in-hand. An existing Task View for an object type might be suitable for your workflow design or it might need slight changes. For example, if an assignee has to set a date field during a task, ensure that the date field is in the Task View. If no existing Task View is suitable for the workflow, you can create a new one.

For information about what Task View is used by a workflow, see [“Defining a standard stage” on page 519](#).

You can add workflow fields to a Task View. For information, see [“System workflow fields” on page 502](#).

The **Actions** button that is defined in an action in a workflow takes precedence over the **Actions** button defined in a Task View.

Consider how to use Task View Overrides per stage when you plan fields, sections, user guidance, and key fields. You can use Task View Overrides to:

- Override whether a field is hidden or read only for a stage.
- Hide a section in a Task View or override the **Initially Collapsed** setting.
- Override the user guidance that is defined in a Task View with user guidance defined for a stage.
- Add the key fields that are defined in the Task View Overrides on a stage to the list of Key Fields in the user guidance panel, regardless of whether the user guidance is defined in the task view or the guidance text override.

An overall design decision you may want to take is to use one Task View in many workflow stages. To do this, do not define user guidance in the Task View. Then, define highly specific user guidance in the Task View Overrides for each stage. Then you can more precisely control the user guidance that are displayed for each stage. And you have fewer Task Views to manage.

An overall design decision you may want to take is to omit key fields from the user guidance in the Task Views. Instead, define key fields in the Task View Overrides on stages. You can then more precisely control the key fields that are displayed for each stage.

Plan the Grid Views for the bulk workflow actions

If you are using the bulk workflow actions feature, determine if existing Grid Views are adequate or whether you must define unique Grid Views. For more information, see [“Defining Grid Views for bulk workflow actions”](#) on page 390.

Review sample workflows

OpenPages provides sample workflows that you can use as delivered or modify to meet your requirements. They can also be used as templates and learning tools for your own workflow. For more information, see the *IBM OpenPages with Watson Solutions Guide*.

Leverage the Preference objects

Review your organization's implementation of Preference objects. You can use Preference objects to hold entity-specific variable values that enable different behavior for different workflows.

- The assignee can be retrieved from the Preference object.
- The oversight user can be retrieved from the Preference object.
- Conditions on an action can be based on a Preference object.

Review the association of Preference objects to Business Entities. If a Business Entity has more than one Preference object associated to it, even if only one is active, a workflow that references fields on the Preference objects will fail. In this situation the following error is issued: **Multiple Preference objects on same entity causes workflow to fail: OP-08521**. To resolve this issue, ensure that only one Preference object is associated to a Business Entity.

For more information about Preference objects, see the *IBM OpenPages with Watson Solutions Guide*.

Plan the due dates

A workflow has an overall due date and each state has a due date. For information, see [“Interpreting and viewing due dates”](#) on page 505.

Using the GRC Workflow Designer

The GRC Workflow Designer is a graphic interface that you use to define, publish, and manage workflows.

To open the GRC Workflow Designer, access the Task Focused UI and click  > **System Configuration > Workflows**. Whether the menu item is displayed depends on your access permissions.

Workflow List

The Workflow List shows workflows that are defined in the Task Focused UI. From the Workflow List, you can:

- Click a workflow. The GRC Workflow Designer opens and you can view or make changes to the workflow.
- Click a column header to change the sort order of the list.
- Select the check box next to a single workflow or multiple workflows to update numerous workflows. The bulk update options are:
 - Delete
 - Enable
 - Disable

Clear the check boxes to hide the bulk update options.

- Select the check box next to a single workflow and click **Start Workflow** to start a workflow for numerous objects at once. It is not possible to start multiple workflow at once.

For more information, see [“Starting workflow instances in bulk” on page 546](#).

- Click **Add New** to create a new workflow. After you define the initial properties, the GRC Workflow Designer opens. For more information, see [“Defining a workflow” on page 513](#).

GRC Workflow Designer components

The GRC Workflow Designer has the following components:

- Canvas

The canvas is where you draw a workflow, create stages, and connect stages with actions.

- Toolbar

Icons on the toolbar allow you to create stages and control the view and the behavior of the canvas.

- Stage and action list panel

The stage and action list panel shows all stages and actions in the workflow. It can be displayed or hidden.

- Property panel

The content of the property panel changes depending on what you select on the canvas. It can be the workflow properties, a selected stage's properties, or a selected action's properties.

The following example shows the GRC Workflow Designer components with the stage and action list hidden.

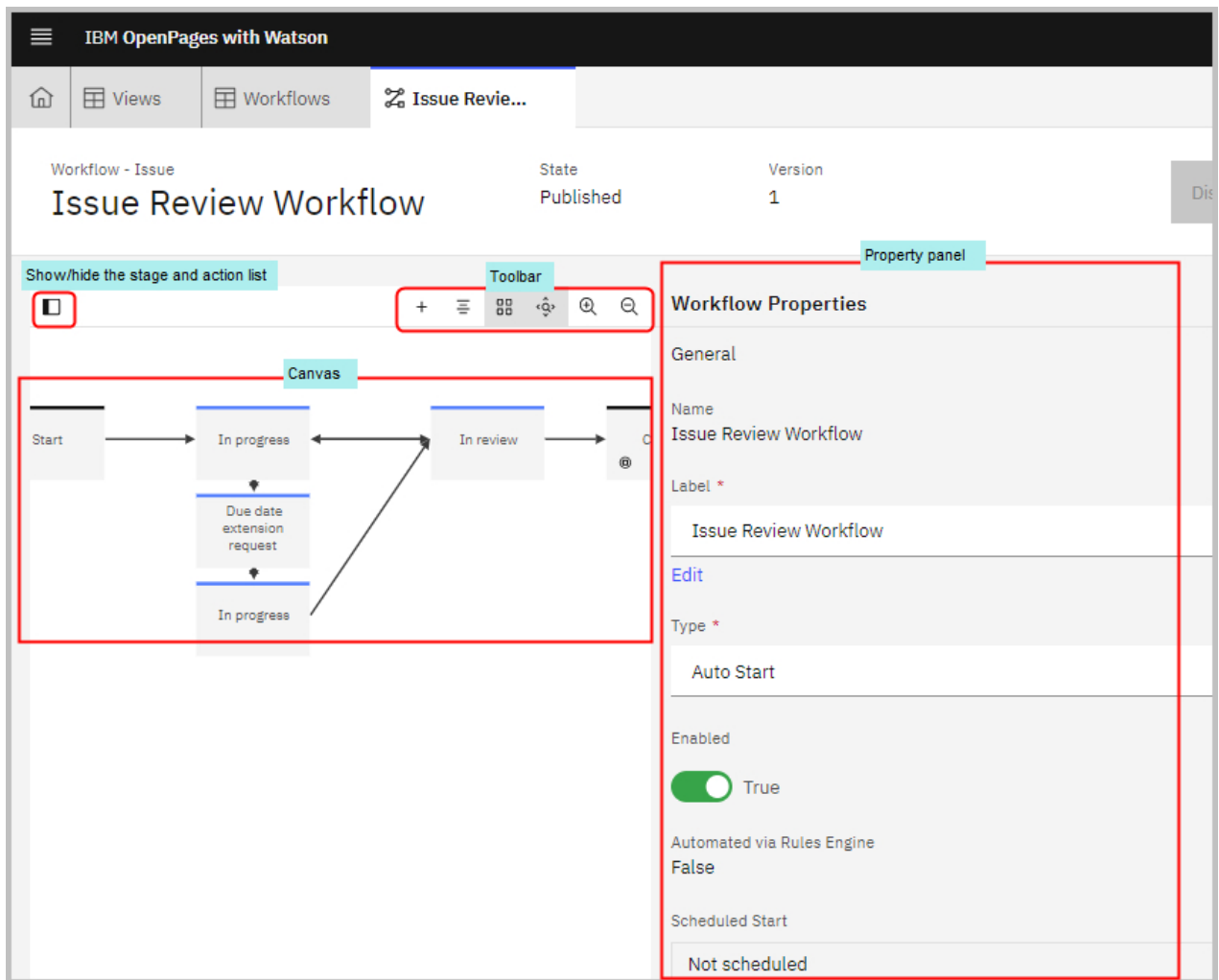


Figure 54. GRC Workflow Designer components

The following example shows the GRC Workflow Designer with the stage and action list displayed.

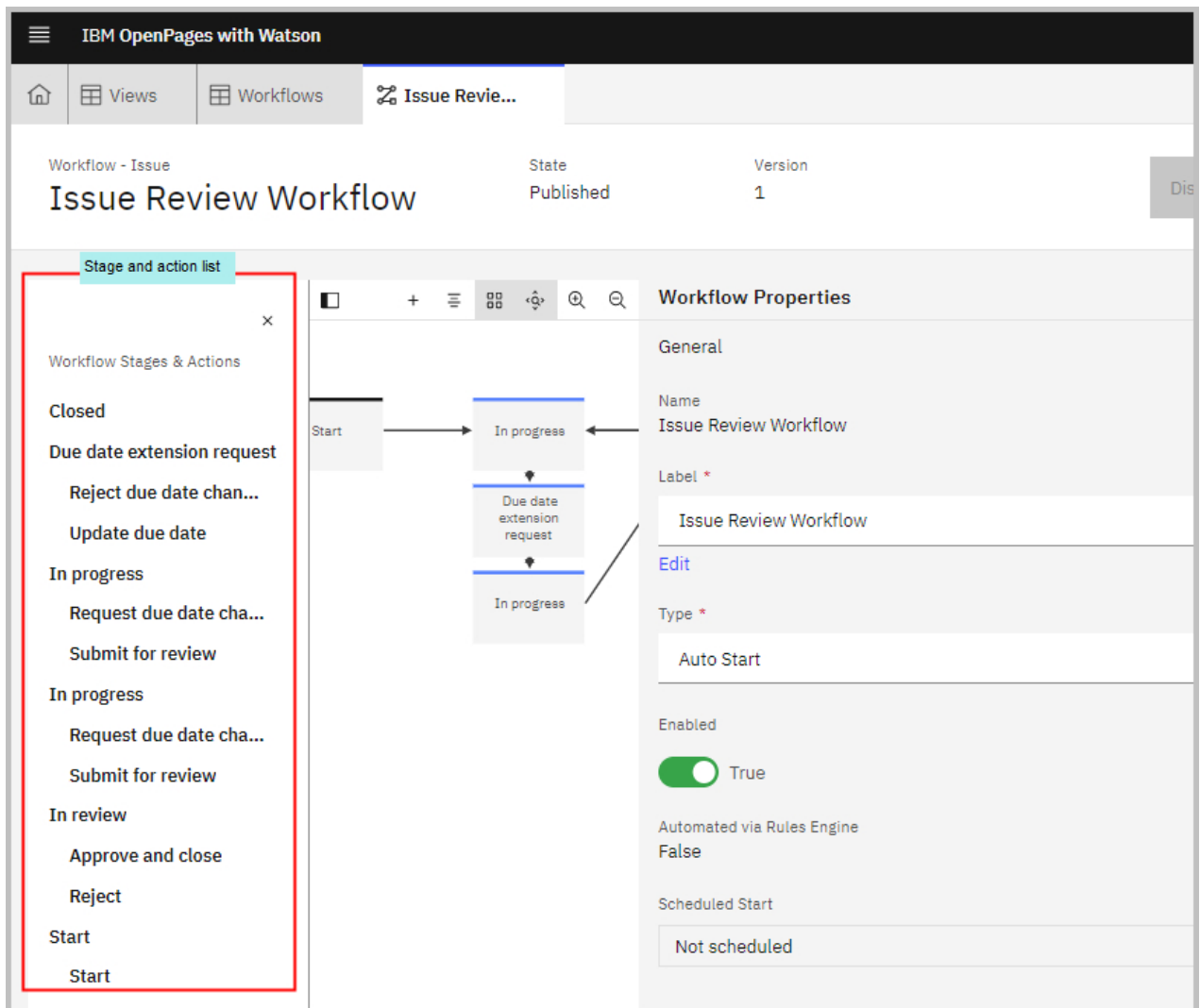


Figure 55. Stage and action list panel in the GRC Workflow Designer

The GRC Workflow Designer contains the following icons:

Table 184. Icons in the GRC Workflow Designer	
Icon	Description
+	Creates a new stage.
≡	Centers the workflow on the canvas.
⊞	Turns on or off snap to grid.
🔍	Turns on or off the mouse zoom.
🔍	Expands (zooms in) the view of the workflow.
🔍	Shrinks (zoom out) the view of the workflow.
📄	Shows or hides the stage and action list panel

How to access the workflow properties for an existing workflow

Click the workflow name that is displayed next to the word *Published* or *Draft* and the version number.

How to create and delete stages

To create a stage, click  and drag it to the canvas.

To delete a stage, you can:

- Select a stage on the canvas and press delete on the keyboard.
- Select a stage on the stage and action list panel and press delete on the keyboard.
- Select a stage on the canvas and click **Remove Stage** in the stage properties panel.

How to create a standard stage

To create a standard stage, click  and drag it to the canvas.

In the stage properties, select *Standard* in **Type**.

For more information, see [“Defining a standard stage” on page 519](#).

How to create an end stage

To create an end stage, click  and drag it to the canvas.

In the stage properties, select *End* in **Type**.

For more information, see [“Defining an end stage” on page 523](#).

How to create and delete actions

To create an action, click the stage where the action starts. Four white points are activated on each side of the stage. Grab a white point and pull a line to the stage where the action ends.

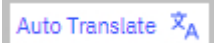
You can connect two stages with one action, for example, an action that represents an approval. The line between the two stages displays with one arrowhead. When you click the line, the properties for the action are displayed in the property panel.

You can also connect two stages with two actions, for example, an action that represents an approval and one that represents a rejection. You draw the first action in one direction, then draw the second action in the reverse direction. The result is a single line with two arrowheads. When you click an arrowhead, the properties for the selected action are displayed in the property panel. Use the property panel to verify that you have the correct action selected.

For more information, see [“Defining a workflow action” on page 527](#).

How to automatically translate workflow, stage, action, and status labels

If it is configured, the [“IBM Watson Language Translator” on page 1018](#) can help you define labels in multiple languages. There are numerous access points in the GRC Workflow Designer.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

How to save a workflow

Your work is automatically saved as you edit a workflow.

How to publish a workflow

Click **Publish** when the workflow is finished.

Each time a workflow definition is published, a new version of that workflow definition is made available to users. The new version is used for workflow instances that are started after it is published. It does not affect workflow instances that are already running.

How to discard a draft version of a workflow

To discard changes you made to a workflow, click **Discard Draft**. All changes since the last published version are discarded.

How to disable a workflow

To disable a workflow, select a workflow from the Workflow List. Select **Disable**.

How to work on a workflow as a team

When you have a workflow open in the GRC Workflow Designer, the URL contains the workflow's internal name. If you are working on the workflow with colleagues, you can send them the URL to share your progress. Although you can collaborate with colleagues, only one user should work on a workflow in the GRC Workflow Designer at a time.

Defining a workflow

A workflow definition contains basic information, stages, and actions.

Before you begin

Complete the follow prerequisites:

- Complete the steps listed in [“Setting up GRC Workflow” on page 495](#).
- Learn about how to use the GRC Workflow Designer. For more information, see [“Using the GRC Workflow Designer” on page 508](#).
- Learn about the Scheduler. For more information, see [“Managing jobs ” on page 551](#).
- Design the workflow. For more information, see [“Designing a workflow” on page 505](#).
- Review the Task View that the workflow uses and make sure it has the content you need. For information, see [“Planning the Task Views” on page 380](#).

Procedure

1. Click  > **Solution Configuration** > **Workflows**.
2. Click **Add New**.
3. Complete the following workflow properties and click **Add**.
 - a) Leave **Enabled** selected. It can be changed later.
 - b) Enter an internal **Name** for the workflow. It cannot be changed later.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
 - c) Select an **Object Type**. It cannot be changed later.
 - d) Select Auto Start or Manual in **Type**. It can be changed later.

For more information, see [“Defining workflow properties ” on page 514](#).

The workflow canvas opens with one default stage, the start stage. The word *Draft* and the version number, *v1*, are displayed next to the workflow name. You can begin defining the workflow.

4. Leave the start stage. A workflow can have only one start stage. Click **Edit** next to **Label** to add labels to the start stage.
5. Define the standard stages.
For information, see [“Defining a standard stage” on page 519](#)
6. Define the end stages.
For information, see [“Defining an end stage” on page 523](#).
7. Connect the stages with actions. For more information, see [“Defining a workflow action” on page 527](#).

Note: You can define a stage and not connect it with an action to another stage. It is not considered an error in the workflow definition. However, the stage is not processed by the workflow. You can use this feature, for example, to define draft stages and workflow branches that you want to save for future use.

8. When you are ready to test the workflow, click **Publish**.

The *v1* version of the workflow becomes the first published version of the workflow.

If the workflow is defined with a scheduled start, a job for the workflow is automatically added to the Scheduler as a job. The job name is a concatenated value of the workflow name, the object type, and - Scheduled Start. A schedule on a workflow cannot be changed in the Scheduler. But you can enable, disable, and start the job. On the linked detail page, you can change the description and view the schedule.

9. Test the workflow. If you need to make changes to the workflow, open it again in the GRC Workflow Designer. Since you are now opening a published workflow, the word *Published* appears, the version number is displayed next to the workflow name and the **Publish** button is grayed out. When you make a change to the workflow, *Published* changes to *Draft*, the version number is incremented by 1, and the **Publish** button becomes active.

To discard changes you make to a workflow, click **Discard Draft**. All changes since the last published version are discarded.

Note: Each time you change the workflow, you need to publish it and re-test it.

It might be helpful to turn on trace logging for workflow during testing and error resolution. For information, see [“Enabling trace logging” on page 829](#).

Defining workflow properties

A workflow has a set of properties that control its overall functionality.

Before you begin

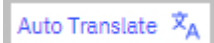
Define basic information (name and object type) for the workflow. For more information, see [“Defining a workflow” on page 513](#).

Procedure

1. Click  > **Solution Configuration** > **Workflows**.
2. Click the workflow that you want to edit.
The GRC Workflow Designer opens.
3. Click anywhere in the empty area of the canvas.
The Workflow Properties panel opens. All of the properties can be edited except **Name** and **Object Type**, which is hidden.
4. Enter a **Label** for the workflow.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

If the workflow is used in multiple locales, enter a workflow label for each language.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

Workflow labels are displayed on the dashboard, My Tasks tab, Subscription Tasks tab, and Oversight Tasks tab.

5. Define how the workflow is launched in **Type**:

- **Auto Start**

The workflow is launched automatically when an object of the object type is created, either by creating new or creating a copy of another object. During a copy, a workflow starts for the main object that is created but not for sub-objects that are created.

- **Manual Start**

The workflow is launched when a user accesses the object and clicks an option on the **Actions** button.

6. Set **Enabled** to true or false. Only enabled workflows can be started.

7. Click **Edit** next to **Scheduled Start** to set up a repeatable schedule. Otherwise, leave **Schedule** set to Not scheduled.

a) Enter a **Name**.

The **Name** displays in the Scheduler as the **Schedule Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

b) Enter a **Description** (optional).

c) Select a schedule type in **Define Schedule**:

- Recurring
- Specified Date/Time
- Cron Expression

d) If you chose Recurring:

- Select a value in **Repeat** (Daily, Weekly, Monthly, Quarterly) and add details such as day, month, or quarter.
- Enter a **Time of Day**.
- Select an **End Date** (optional).

e) If you chose Specified Date/Time:

- Select a **Date**.
- Enter a **Time of Day**.

f) If you chose Cron Expression:

- Enter a **Cron Expression**.
- Select an **End Date** (optional).

Advanced users can choose a cron expression if a Recurring or Specified Date/Time schedule does not meet your needs. Use the syntax for cron expressions, not crontab expressions.

g) Click **Done**.

8. Set **Execute As System** to false to execute the workflow as the logged in user. Set **Execute As System** to true to execute the workflow as the OPSsystem user. The workflow can then perform operations that the logged in user cannot. Change history shows OPSsystem as the user who performed the action.

9. Set **Automated** to true or false. Automated workflows do not have standard stages, only start and end stages. They are used in IBM OpenPages Regulatory Compliance Management. For more information, see “Processing regulatory events by using rules” on page 1060.
10. Designate the **Oversight** users. These are users in the organization who have oversight responsibility for activity that is generated by the workflow. Their work is summarized on the Oversight Tasks tab. You can select only actor fields. Do not select a system workflow field such as *System Workflow Fields:Overseers*. You can assign multiple oversight users to a workflow. They can be from multiple sources, for example, a specific user, a field on the current object, and a field on a related object.

a) Click **Add Oversight**. In **Assign To** choose what value to set the oversight user to:

- **Users or Groups**
- **A field in the current object**
- **A field in a related object**
- **A field in a preference object**

The panel changes depending on your selection.

b) Complete the panel.

c) Click **Done**.

11. Define how the **Overall Due Date** for the workflow is determined.

In **Assign To** choose what value to set the overall due date to:

- **Workflow Start Date** (the date the workflow instance starts)
- **A specified value**
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- **A field in the Preference object**

You can optionally add **Filter By** conditions.

In **Adjust Date By** you can optionally define an offset for the date you chose in **Assign To**. The offset can be:

- **A specified value** and enter **Number of Days**.
- **A field in the current object**
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- **A field in the Preference object**

You can optionally add **Filter By** conditions.

12. In **Applicability** you define the conditions under which the workflow starts. Expand **Applicability** and click **Add Condition**. The **Applicability** panel opens.

- Leave blank if only one workflow is defined for the object type and if any user can start the workflow without restriction.
- Add conditions if multiple workflows are defined for the object type. The conditions in **Applicability** determine which workflow is started for a specific object. **Applicability** is especially important if **Type** is set to *Auto start*.
- Add a condition if you want to restrict who can start the workflow. The condition determines which users or user groups are allowed to start the workflow. Without this condition, any user can start the workflow.
- Add a date condition to additionally restrict a workflow that starts on a schedule (optional). For example, define a condition that Review Date must be equal to today. Like all workflows, a workflow that is defined to start on a schedule must meet the **Applicability** conditions to start.
- For each condition, you build a comparison statement with two fields and an operator.
- If you define multiple conditions, all conditions must be met for the workflow to start.

To override this rule, define **Advanced Logic** to combine the conditions in a specific way.

- a) In **Compare** you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is (or is not) a specified user or is (or is not) in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

- b) In **Using** choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

- c) In **To** you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**.

- **An expression**

Enter a single field or variable from the list in [“Using variables, functions, and fields”](#) on page 503. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name

like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

Note: An object's system comment field (System Fields:Comment) cannot be used in a field comparison in a condition.

d) If you chose a date field in **Compare**, you can optionally define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can optionally add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

13. Define the **Criticality**. Select a single value enumerated field that contains the criticality of the object type for this workflow, and map its values to standard values (low, medium, high, and critical).

Each object type in OpenPages can use a different field for criticality. When you map the object fields to standard values, you normalize the values across object types. When criticality fields are displayed on a dashboard, the normalized values can then provide consistent information across object types.

Workflow stages

A workflow is made up of one start stage, one or many standard stages, and one or many end stages.

Defining a standard stage

A workflow can have one or many standard stages.

Procedure

1. Click  > **Solution Configuration** > **Workflows**.

2. Click the workflow that you want to edit.

The GRC Workflow Designer opens.

3. Click  in the toolbar and drag it to the canvas.

4. In the **Add Stage** window, give the stage a **Name** and click **Add**.

This is an internal name and it cannot be changed later. In the next step, you can define a label for the stage.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

Maximum length is 40 characters. Keep the stage names short.

5. Enter a **Label** for the stage.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

The label is populated to all languages.

If the workflow is used in multiple locales, enter a stage label for each language.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

Maximum length is 40 characters.

Keep the stage labels short, for example, In Progress, In Review, In Approval, and Closed. Stage labels are displayed in the workflow information card.

6. Choose Standard in **Type**.

7. In **Access Control** (access control overrides for non-participants) define whether non-participants can view and edit objects at this stage.

Access for participants (assignees, oversight users, and subscribers) and non-participants is based on access control that is defined on the role template that a user is assigned to. Only participants can access the **Actions** button.

In **Access Control** define whether to override access controls for non-participants.

- **Strict**

Override non-participants' access control and do not allow them to view a task at this stage.

- **Read**

Override non-participants' access control and allow them to view but not edit a task at this stage.

- **Open**

Override non-participants' access control and allow them to view and edit a task at this stage.

- **No Override**

Do not override non-participants' access control. Grant access to view and edit a task at this stage based on access control that is defined on the role template that the user is assigned to.

8. In **Due Date** define the stage due date.

In **Assign To** choose how the stage due date is set.

- Start Date (the date when a workflow instance enters (or re-enters) the stage)
- A specified value
- A field in the current object
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- A field in a Preference object

You can optionally add **Filter By** conditions.

In **Adjust Date By** you can optionally define an offset for the date you chose in **Assign To**. The offset is always in days and can be negative. It can be:

- A specified value, for example, 10 days.
- A field in the current object
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- A field in a Preference object

You can optionally add **Filter By** conditions.

Expand **Assignees and Subscribers** to designate the assignees and subscribers for tasks at this stage.

You can select only actor fields. Do not select a system workflow field such as *System Workflow Fields:Assignees*. You can assign multiple assignees and multiple subscribers to a stage. They can be from multiple sources, for example, a specific user, a field on the current object, and a field on a related object.

9. Click **Add Assignee** to designate the assignees for tasks at this stage. You can choose to:

Assign to

- Users or groups
- A field in the current object
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- A field in a preference object

You can optionally add **Filter By** conditions.

10. Click **Add Subscriber** to designate the subscribers for tasks at this stage. You can choose to:

Assign to

- Users or groups
- A field in the current object
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- A field in a Preference object

You can optionally add **Filter By** conditions.

11. Set **Enable Reminders** to true to send email reminders. Configure who receives reminders and when.

- Set **Send reminders to Assignees** to true or false.
- Set **Send reminders to Subscribers** to true or false.
- Configure how frequently email reminders are sent in the following settings.

Table 185. Reminder frequency settings		
Setting	Description	Example
Send reminder __ day(s) before due date	A user receives one email reminder x days before the due date.	1= user receives one email reminder one day before the due date
	Do not enter 0. Instead, set Send reminders on due date to true.	3= user receives one email reminder three days before the due date

Table 185. Reminder frequency settings (continued)

Setting	Description	Example
Send reminder every __ day(s) until due date	A user receives repeating email reminders every x days until the due date.	1= user receives an email reminder every day until the due date 3= user receives an email reminder every three days until the due date
Send reminders on due date (true/false)	If true, a user receives one email reminder on the due date.	
Send reminder every __ day(s) for overdue tasks	A user receives repeating email reminders every x days after the due date has passed. Emails are sent until the stage is completed.	1= user receives an email reminder every day after the due date has passed 3= user receives an email reminder every three days after the due date has passed

In **Bulk Workflow Action** to configure bulk workflow actions.

12. Set **Bulk Workflow Action** to true to enable bulk workflow actions.
13. Select a Grid View in **Select a grid view for Bulk Workflow Action**. For more information, see [“Defining Grid Views for bulk workflow actions”](#) on page 390.
14. In **Enable Workflow Actions for Bulk Processing**, each action in the workflow is displayed. Turn on each action that you want to allow users to take during bulk workflow actions. Each activated action will be an option in the toolbar in the Grid View.

Expand **Task View Overrides** to provide overrides that customize the Task View that is displayed to the user for the stage.

15. In **View** select a task view for the stage or leave blank.

If you provide a task view, you can also provide field, section, and user guidance overrides that customize the task view for the stage. The task view must be enabled.

If blank, the system uses information in the workflow and rules on the task views for the object type to determine the task view that is displayed.

16. In **Fields** define field overrides for the task view. Click **Add Field**, choose a field, and set the following attributes:

- **Hidden** (true or false) overrides rules in the task view that determine whether the field is shown or hidden.
- **Read Only** (true or false) overrides rules in the task view that determine whether a field is read only.
- **Key Field** (true or false) adds the field to the list of Key Fields in the user guidance panel, regardless of whether the user guidance is defined in the task view or the guidance text override.

If a field is hidden in a view due to a task view override, it is also hidden in the user guidance panel if it is defined as a key field.

For more information about key fields, see [“Adding user guidance”](#) on page 402.

17. In **Sections** define section overrides for the task view (optional). Click **Add Section**, choose a section, and set the following attributes:

- **Hide Section** (true or false) controls whether the section is shown or hidden.
- **Initially Collapsed** (true or false) overrides the **Initially Collapsed** setting that is defined on the section in the task view.

For more information about sections, see [“Adding a section” on page 399](#).

18. Enter a **Guidance Title** to provide a title for the user guidance panel for the stage. The title is populated to all languages. Alternatively, you can enter titles for different languages.
19. Enter **Guidance Text** to override the user guidance text on the task view. The text is populated to all languages. Alternatively, you can enter user guidance text for different languages. For more information about user guidance, see [“Adding user guidance” on page 402](#).

Defining an end stage

A workflow must have at least one end stage.

Procedure

1. Click  > **Solution Configuration** > **Workflows**.

2. Click  in the toolbar and drag it to the canvas.

3. In the **Add Stage** window, give the stage a **Name** and click **Add**.

This is an internal name and it cannot be changed later. In the next step, you can define a label for the stage.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

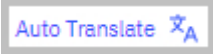
Maximum length is 40 characters. Keep the stage names short.

4. Enter a **Label** for the stage.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

The label is populated to all languages.

If the workflow is used in multiple locales, enter a stage label for each language.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

Maximum length is 40 characters.

Keep the stage labels short, for example, In Progress, In Review, In Approval, and Closed. Stage labels are displayed in the workflow information card.

5. Choose End in **Type**.

In **End Stage Notifications** designate who receives an email notification when the workflow ends.

6. Add other users who receive email notifications.

- a) Click **Add User**.

You can assign to:

- **Users or groups**
- **A field in the current object**
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Add **Filter By** conditions (optional).

- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- **A field in a preference object**

You can optionally add **Filter By** conditions and set **Advanced Logic**.

The panel changes depending on your selection.

- Complete the panel.
- Click **Done**.

In **Operations** click **Add Operation** to define an operation that executes when the workflow ends. The only operation that is available is to start a workflow.

- In **Operation** choose **start a workflow**. When the current workflow ends, another workflow immediately begins for the same object.
- Provide a **Name** for the operation.
- Click **Add Condition** to add one or more conditions to the **start a workflow** operation. The **When** panel opens. For each condition you build a comparison statement with two fields and an operator.
 - In **Compare** you define the first field in the comparison statement. You can choose:
 - **A field in the current object**
Select an **Object Field**.
 - **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
 - **A field in a Preference object**
Select a **Preference Object Field**. You can optionally add **Filter By** conditions.
 - **End User**
An **End User** condition checks whether the signed on end user is (or is not) a specified user or is (or is not) in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.
 - In **Using** choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.
 - In **To** you define the second field in the comparison statement. You can choose:
 - **A specified value**
The value that you can provide depends on the field type of the field you chose in **Compare**.
 - **An expression**
Enter a single field or variable from the list in “Using variables, functions, and fields” on page 503. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.
 - **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

Note: An object's system comment field (System Fields:Comment) cannot be used in a field comparison in a condition.

d) If you chose a date field in **Compare**, you can optionally define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can optionally add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

10. **Target Objects** defaults to Self and cannot be changed.

11. In **Workflow** enter the name of the workflow to start. The workflow must be for the same object type as the workflow that is ending. It must be published.

12. Click **Done**.

Workflow actions

Actions control aspects of the transition to the next or previous stage.

Conditions and validations

You use conditions and validations to customize the presentation to the user and to define the behavior of a workflow. The options for conditions and validations are the same. The difference between conditions and validation is their effect on the behavior of the Task View when a user completes their work.

- Conditions control whether an action is visible or hidden on the **Actions** button. Examples include:
 - You can define a condition that displays **Escalation** on the **Actions** button if the loss amount is greater than \$1M.
 - You can define a condition that hides **Submit** on the **Actions** button if given fields are empty.
 - You can define a condition that hides **Submit** on the **Actions** button if all related action items are not closed.

Conditions provide a means for you to restrict the options that are available to users and, thereby, hide parts of the workflow. For example, you can use conditions to control when a workflow branches. Say that you have two types of issues, IT and OR, and each issue type has an approval process. The workflow branches based on the issue type but the button is always labeled **Submit**. The workflow takes the correct branch based on the condition. The user follows the workflow for their issue type and is unaware of the other issue type.

- Validations check that an object has specific attributes for the action to complete. If the validation fails, an error is displayed and the user must take corrective steps. Examples include:
 - You can define a validation that makes certain fields mandatory when the user clicks **Escalation**. If the fields are empty, an error is displayed. The user must provide values to continue.
 - You can define a validation that requires all related action items be closed. If they are not closed, the user must close them to continue.

Operations

Operations control what is done when the action completes. For example, when an object is approved, you can create an object, start another workflow, or set a date field to today's date or a user field to the user who finished the action.

An action can complete the following types of operations:

- Create objects
- Execute a custom action
- Lock or unlock objects
- Set fields
- Start a workflow

Order of validations and operations

Validations and operations are performed in the order given. For example, an action can perform a validation, then an operation, and then another validation.

Initial and final actions

The first action in a workflow is from the start stage to the first standard stage. This action occurs automatically without user input. You can use this action to define initial properties for the workflow. If there are multiple first standard stages, each action from the start stage to the standard stage must have a condition.

The final action in a workflow is from the last standard stage to the end stage. You can use this action to reset any field values, if needed, and to define fields you need for the next workflow, if there is one.

Defining a workflow action

About this task

You can connect two stages with one action, for example, an action that represents an approval. The line between the two stages displays with one arrowhead. When you click the line, the properties for the action are displayed in the property panel.

You can also connect two stages with two actions, for example, an action that represents an approval and one that represents a rejection. You draw the first action in one direction, then draw the second action in the reverse direction. The result is a single line with two arrowheads. When you click an arrowhead, the properties for the selected action are displayed in the property panel. Use the property panel to verify that you have the correct action selected.

In **Validations and Operations** you can add one or more validations and one or more operations. They are performed in the order given. Drag the validations and operations up or down to place them in the correct order for processing.

Procedure

1. Click  > **Solution Configuration** > **Workflows**.

2. Click the workflow that you want to edit.

The GRC Workflow Designer opens.

3. To create an action, click the stage where the action starts. Four white points are activated on each side of the stage. Grab a white point and pull a line to the stage where the action ends.
4. In the **Add Action** window, keep the default or give the action a **Name** and click **Add**.

This is an internal name and it cannot be changed later. The name must be unique within a stage. In the next step, you can define a label.

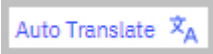
Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

The **Action Properties** panel opens.

5. In **Label** enter a label for the action. The default is the **Name**.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

The **Name** is populated to labels for other languages. Click **Edit** and overwrite the labels if the workflow is used in multiple locales.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

Workflow labels are displayed on the dashboard, My Tasks tab, Subscription Tasks tab, and Oversight Tasks tab.

Action labels are displayed as options under the **Actions** button.

Keep the action labels short, for example, Submit for review, Reject, Send for approval, Reject approval, and Approve and close.

6. In **Status** enter a status that is assigned to the next stage in the workflow. The value is populated to all languages. Alternatively, choose a language and enter a value for that language. You can enter values for multiple languages.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

Statuses display in the workflow information card as stage label [status label], for example, *In Review* [*Rejected*]. There is one exception to this rule and that is the action to the end stage. The status of the end stage is not displayed in the information card.

There is no automatic link between the **Status** field on a workflow and any status fields that can exist on an object, for example, the Business Continuity Plan status field (BC-Plan:Status). Use a **set fields** operation on an action to control the value in object status fields as objects move through a workflow.

7. In **Comment** you can control how the action handles a user-entered comment. Options are:

- **None** - no comment is allowed and a comment window is not displayed.
- **Optional** - a comment window is displayed and a user can enter a comment. However, the comment is not required for the action to complete.
- **Required** - a comment window is displayed and a user must enter a comment for the action to complete.

The **Comment** setting is hidden for the initial action in a workflow (from the start stage to the first standard stage).

8. In **Override workflow action text** provide text that displays on the confirmation window that users interact with. For more information, see [“Confirm the selected action” on page 501](#).

9. Set **Run in Background** to **True** if the action is expected to take a long time.

10. In **Email** set the following options to **True** to send email notifications when the action completes:

- **Notify Assignees**
- **Notify Subscribers**

If **Run in Background** is set to **True**, email notifications are sent regardless of how **Email** is defined.

11. Expand **Conditions** and click **Add Condition**. The **Conditions** panel opens.

Conditions control whether an action is visible or hidden on the **Actions** button. Conditions provide a means for you to restrict options available to users and hide the workflow and its complexity.

You can add one or more conditions. For each condition you build a comparison statement with two fields and an operator.

All conditions must be met for the action on the **Actions** button to display.

To override this rule, define **Advanced Logic** to combine the conditions in a specific way.

a) In **Compare** you define the first field in the comparison statement. You can choose:

- **A field in the current object**
Select an **Object Field**.
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is (or is not) a specified user or is (or is not) in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

b) In **Using** choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

c) In **To** you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**.

- **An expression**

Enter a single field or variable from the list in [“Using variables, functions, and fields”](#) on page 503. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

Note: An object's system comment field (System Fields:Comment) cannot be used in a field comparison in a condition.

d) If you chose a date field in **Compare**, you can optionally define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can optionally add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

12. Expand **Validations and Operations** and click **Add Validation** to define a validation. The **Validations** panel opens.

Validations check that an object has specific attributes for the action to complete. If the validation fails, an error is displayed and the user must take corrective steps.

All validations must be met for the action to complete. For each validation you build a comparison statement with two fields and an operator.

a) In **Compare** you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is (or is not) a specified user or is (or is not) in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

b) In **Using** choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

c) In **To** you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**.

- **An expression**

Enter a single field or variable from the list in [“Using variables, functions, and fields”](#) on page 503. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name

like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

Note: An object's system comment field (System Fields:Comment) cannot be used in a field comparison in a condition.

d) If you chose a date field in **Compare**, you can optionally define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can optionally add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

13. Expand **Validations and Operations** and click **Add Operation** to define an operation. The **Operations** panel opens.

Operations define what is done when the action completes.

If you provide multiple operations, all operations are performed.

a) In **Operation** choose an operation type. Valid values are:

- Create objects
- Custom action
- Lock or unlock objects
- Set fields
- Start a workflow

The fields on the **Operations** panel change depending on the operation type you choose.

b) Follow the instructions for the operation type. For more information see:

- [“Defining a workflow action that creates objects” on page 532](#)
- [“Defining a workflow action that runs a custom action ” on page 535](#)
- [“Defining a workflow action that locks or unlocks objects” on page 537](#)
- [“Defining a workflow action that sets fields” on page 539](#)
- [“Defining a workflow action that starts a workflow” on page 542](#)
- [“Defining a workflow action that runs a calculation” on page 544](#)

14. If you provide multiple validations or operations, review the order. Validations and operations are executed in the order given.

What to do next

Depending on the workflow, you might need to define an action back to the previous stage.

Repeat the step of creating an action but in the reverse direction. The result is a single line with two arrowheads. When you click an arrowhead, the properties for the selected action are displayed in the property panel. Use the property panel to verify that you have the correct action selected.

Defining a workflow action that creates objects

A **create objects** operation on an action creates a single direct child object.

Before you begin

Define a workflow and add stages and actions to it. For information about how to define an action, [“Defining a workflow action” on page 527](#).

Review [“Designing a workflow” on page 505](#). Be aware of the potential of creating an infinite loop when defining a workflow action that creates objects.

Procedure

1. In the GRC Workflow Designer, click the action that you want to edit.

The **Action Properties** panel opens.

2. Expand **Validations and Operations**.

3. Click **Add Operation**. The **Operations** panel opens.

4. Set **Operation** to **create objects**.

5. Provide a **Name** for the operation.

6. Next to **When**, click **Add Condition** to define one or more conditions. The **When** panel opens.

All conditions must be met for the operation to complete. For each condition you build a comparison statement with two fields and an operator.

a) In **Compare** you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is (or is not) a specified user or is (or is not) in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

b) In **Using** choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

c) In **To** you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**.

- **An expression**

Enter a single field or variable from the list in “Using variables, functions, and fields ” on page 503. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$] .pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

Note: An object's system comment field (System Fields:Comment) cannot be used in a field comparison in a condition.

d) If you chose a date field in **Compare**, you can optionally define an offset in **Adjust Date By** .

- **A specified value** and enter **Number of Days**.

- **A field in the current object**
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
- **A field in the Preference object**

You can optionally add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

7. Set **Execute As System** to false to execute the action as the logged in user. Set **Execute As System** to true to execute the action as the OPSsystem user. The action can then perform operations that the logged in user cannot. Change history shows OPSsystem as the user who performed the action.
8. Choose a **Related Object Type**. You can choose only from child object types of the object type for the workflow.
9. Enter an **Object Name** to assign to the newly created object. It is not displayed for all object types or if auto naming is enabled. If auto naming is not enabled, once a workflow creates an object the workflow cannot be started again for the same object.

Tip: If **Object Name** is displayed, you can add the [\$TODAY\$] expression to make it unique per day. For example, if you enter Auto_Issue_[\$TODAY\$], the newly created object is named Auto_Issue_07182019.

10. Add **Fields** and set their values on the newly created object.

11. Click **Done**.

Results

When the action takes place, a new object is created and the workflow continues to the next stage. If an auto-start workflow exists for the child object type and the applicability conditions are met, a workflow starts for the newly created object. Both workflow, the one for the parent and the one for the child, continue and are independent of each other.

Defining a workflow action that runs a custom action

Use **custom action** to define custom business logic for an action.

Before you begin

Define a workflow and add stages and actions to it. For information about how to define an action, [“Defining a workflow action” on page 527](#).

About this task

Custom actions are a means to implement workflows that have similar functionality to triggers in OpenPages. The action is evaluated during an action and `customaction` class is instantiated and executed.

For more information, see [Appendix F, “Creating custom actions for GRC workflows,” on page 1117](#).

Procedure

1. In the GRC Workflow Designer, click the action that you want to edit.

The **Action Properties** panel opens.

2. Expand **Validations and Operations**.

3. Click **Add Operation**. The **Operations** panel opens.

4. Set **Operation** to **custom action**.

5. Provide a **Name** for the operation.

6. Next to **When**, click **Add Condition** to define one or more conditions. The **When** panel opens.

All conditions must be met for the operation to complete. For each condition you build a comparison statement with two fields and an operator.

- a) In **Compare** you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is (or is not) a specified user or is (or is not) in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

- b) In **Using** choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

- c) In **To** you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**.

- **An expression**

Enter a single field or variable from the list in [“Using variables, functions, and fields”](#) on page 503. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

Note: An object's system comment field (System Fields:Comment) cannot be used in a field comparison in a condition.

d) If you chose a date field in **Compare**, you can optionally define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can optionally add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
 - 1 and (2 or 3)
 - 1 not (2 or 3)
7. Set **Execute As System** to false to execute the action as the logged in user. Set **Execute As System** to true to execute the action as the OPSysSystem user. The action can then perform operations that the logged in user cannot. Change history shows OPSysSystem as the user who performed the action.
 8. Enter a **Class Name**.
 9. You can provide one or more properties. A property is a Name/Value pair. An example of a Name/Value pair is ObjectType/SOXPProcess. Both Name and Value must be strings.
 10. Click **Add Fields** and designate fields that are passed to the custom action.
 11. Click **Done**.

Defining a workflow action that locks or unlocks objects

A **lock or unlock objects** operation on an action locks or unlocks either the object that a workflow is processing or one or more related objects.

Before you begin

Define a workflow and add stages and actions to it. For information about how to define an action, [“Defining a workflow action” on page 527](#).

Procedure

1. In the GRC Workflow Designer, click the action that you want to edit.
The **Action Properties** panel opens.
2. Expand **Validations and Operations**.
3. Click **Add Operation**. The **Operations** panel opens.
4. Set **Operation** to **lock or unlock objects**.
5. Provide a **Name** for the operation.
6. Next to **When**, click **Add Condition** to define one or more conditions. The **When** panel opens.
All conditions must be met for the operation to complete. For each condition you build a comparison statement with two fields and an operator.
 - a) In **Compare** you define the first field in the comparison statement. You can choose:
 - **A field in the current object**
Select an **Object Field**.
 - **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
 - **A field in a Preference object**
Select a **Preference Object Field**. You can optionally add **Filter By** conditions.
 - **End User**

An **End User** condition checks whether the signed on end user is (or is not) a specified user or is (or is not) in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

b) In **Using** choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

c) In **To** you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**.

- **An expression**

Enter a single field or variable from the list in [“Using variables, functions, and fields”](#) on page 503. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

Note: An object's system comment field (System Fields:Comment) cannot be used in a field comparison in a condition.

d) If you chose a date field in **Compare**, you can optionally define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can optionally add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

7. Set **Execute As System** to false to execute the action as the logged in user. Set **Execute As System** to true to execute the action as the OPSysSystem user. The action can then perform operations that the logged in user cannot. Change history shows OPSysSystem as the user who performed the action.

8. Click **Edit** next to **Target Objects**. Establish what objects are locked or unlocked.

a. Select a **Relationship Type**:

- Self
- Direct Child
- Direct Parent
- Ancestor
- Descendant

b. Select a **Related Object Type** if you chose any value other than Self. The list is filtered based on what you chose in **Relationship Type**.

c. Click **Add Condition** to add a condition to the target object.

d. If you chose Ancestor or Descendant in **Relationship Type**, select a path in **Relationship Paths**.

e. Click **Done**.

9. In **Lock/unlock** choose lock or unlock.

10. Click **Done**.

Defining a workflow action that sets fields

A **set fields** operation on an action sets values for specified fields on either the object that a workflow is processing or one or more related objects.

Before you begin

Define a workflow and add stages and actions to it. For information about how to define an action, [“Defining a workflow action” on page 527](#).

About this task

If a **set fields** operation sets a field on a child object, conditional on another field on that child object, the action works only if all children meet the condition. If any child object does not meet the condition, then no changes are made to any child. A solution for this is to add a **Filter by** condition on the **When** panel so that only a subset of children are included.

An error is issued if a **set fields** operation sets a field on related objects but no related objects exist. A solution for this is to include a condition that confirms that at least one related object exists. For example, include a condition that confirms that a required field, such as Name, is not empty. Such a condition returns false if no related objects exist and, therefore, prevents the operation from being executed.

Procedure

1. In the GRC Workflow Designer, click the action that you want to edit.

The **Action Properties** panel opens.

2. Expand **Validations and Operations**.
3. Click **Add Operation**. The **Operations** panel opens.
4. Set **Operation** to **set fields**.
5. Provide a **Name** for the operation.
6. Next to **When**, click **Add Condition** to define one or more conditions. The **When** panel opens.

All conditions must be met for the operation to complete. For each condition you build a comparison statement with two fields and an operator.

- a) In **Compare** you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is (or is not) a specified user or is (or is not) in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

- b) In **Using** choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

- c) In **To** you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**.

- **An expression**

Enter a single field or variable from the list in [“Using variables, functions, and fields”](#) on page 503. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.

- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
 - **A field in a Preference object**
Select a **Preference Object Field**. You can optionally add **Filter By** conditions.
- Note:** An object's system comment field (System Fields:Comment) cannot be used in a field comparison in a condition.
- d) If you chose a date field in **Compare**, you can optionally define an offset in **Adjust Date By**.
- **A specified value** and enter **Number of Days**.
 - **A field in the current object**
 - **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
 - **A field in the Preference object**
You can optionally add **Filter By** conditions.
- e) Click **Done**.
The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.
- f) Optional: Add more conditions.
- g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.
The order of operations is: () then NOT then AND then OR.
For example:
- 1 or 2 or 3
 - 1 and (2 or 3)
 - 1 not (2 or 3)
7. Set **Execute As System** to false to execute the action as the logged in user. Set **Execute As System** to true to execute the action as the OPSsystem user. The action can then perform operations that the logged in user cannot. Change history shows OPSsystem as the user who performed the action.
8. Click **Edit** next to **Target Objects**. Define what objects contain the fields that will be set.
- a. Select a **Relationship Type**:
- Self
 - Direct Child
 - Direct Parent
 - Ancestor
 - Descendant

- b. Select a **Related Object Type**. The list is filtered based on what you chose in **Relationship Type**.
 - c. Click **Add Condition** to add a condition for setting the field on the target object.
 - d. If you chose Ancestor or Descendant in **Relationship Type**, select a path in **Relationship Paths**.
 - e. Click **Done**.
9. Add **Fields** and set their values on the selected object.
 10. Click **Done**.

Defining a workflow action that starts a workflow

A **start workflow** operation on an action launches a workflow for a related object.

Before you begin

Define a workflow and add stages and actions to it. For information about how to define an action, [“Defining a workflow action” on page 527](#).

Procedure

1. In the GRC Workflow Designer, click the action that you want to edit.
The **Action Properties** panel opens.
2. Expand **Validations and Operations**.
3. Click **Add Operation**. The **Operations** panel opens.
4. Set **Operation** to **start a workflow**.
5. Provide a **Name** for the operation.
6. Next to **When**, click **Add Condition** to define one or more conditions. The **When** panel opens.
All conditions must be met for the operation to complete. For each condition you build a comparison statement with two fields and an operator.
 - a) In **Compare** you define the first field in the comparison statement. You can choose:
 - **A field in the current object**
Select an **Object Field**.
 - **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
 - **A field in a Preference object**
Select a **Preference Object Field**. You can optionally add **Filter By** conditions.
 - **End User**
An **End User** condition checks whether the signed on end user is (or is not) a specified user or is (or is not) in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.
 - b) In **Using** choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.
 - c) In **To** you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page 503. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

Note: An object's system comment field (System Fields:Comment) cannot be used in a field comparison in a condition.

d) If you chose a date field in **Compare**, you can optionally define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can optionally add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

7. Set **Execute As System** to false to execute the action as the logged in user. Set **Execute As System** to true to execute the action as the OPSys user. The action can then perform operations that the logged in user cannot. Change history shows OPSys as the user who performed the action.
8. Click **Edit** next to **Target Objects** to define the object that the workflow is started for.
 - a. Select a **Relationship Type**:
 - Direct Child
 - Direct Parent
 - Ancestor
 - Descendant
 - b. Select a **Related Object Type**. The list is filtered based on what you chose in **Relationship Type**.
 - c. Click **Add Condition** next to **Filter By** to add a condition to the target object.
 - d. If you chose Ancestor or Descendant in **Relationship Type**, select a path in **Relationship Paths**.
9. In **Workflow** enter the name of the workflow to start. The workflow must be for object type designated in **Related Object Type** and it must be published.
10. Click **Done**.

Results

When the action takes place, the new workflow starts. Both workflows continue and are independent of each other.

Defining a workflow action that runs a calculation

A **run a calculation** operation on an action runs a calculation on an object.

Before you begin

Define a workflow and add stages and actions to it. For information about how to define an action, [“Defining a workflow action” on page 527](#).

Define and publish the calculation that the action runs. The calculation type must be manual. For more information, see [“Defining a calculation” on page 467](#).

Procedure

1. In the GRC Workflow Designer, click the action that you want to edit.

The **Action Properties** panel opens.
2. Expand **Validations and Operations**.
3. Click **Add Operation**. The **Operations** panel opens.
4. Set **Operation** to **run a calculation**.
5. Provide a **Name** for the operation.
6. Next to **When**, click **Add Condition** to define one or more conditions. The **When** panel opens.

All conditions must be met for the operation to complete. For each condition you build a comparison statement with two fields and an operator.

 - a) In **Compare** you define the first field in the comparison statement. You can choose:
 - **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is (or is not) a specified user or is (or is not) in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

b) In **Using** choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

c) In **To** you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**.

- **An expression**

Enter a single field or variable from the list in [“Using variables, functions, and fields”](#) on page 503. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

Note: An object's system comment field (System Fields:Comment) cannot be used in a field comparison in a condition.

d) If you chose a date field in **Compare**, you can optionally define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
- **A field in the Preference object**
- You can optionally add **Filter By** conditions.
- e) Click **Done**.
- The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.
- f) Optional: Add more conditions.
- g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.
- The order of operations is: () then NOT then AND then OR.
- For example:
- 1 or 2 or 3
 - 1 and (2 or 3)
 - 1 not (2 or 3)
7. Set **Execute As System** to false to execute the action as the logged in user. Set **Execute As System** to true to execute the action as the OPSysSystem user. The action can then perform operations that the logged in user cannot. Change history shows OPSysSystem as the user who performed the action.
8. Click **Edit** next to **Target Objects** to define the object that the workflow is started for.
- a. Select a **Relationship Type**:
 - Self
 - Direct Child
 - Direct Parent
 - Ancestor
 - Descendant
 - b. Select a **Related Object Type**. The list is filtered based on what you chose in **Relationship Type**.
 - c. Click **Add Condition** next to **Filter By** to add a condition to the target object.
 - d. If you chose Ancestor or Descendant in **Relationship Type**, select a path in **Relationship Paths**.
9. In **Calculation** enter the name of the calculation to start. The calculation must be for the same object type as the workflow, it must be published, and the calculation type must be manual.
10. Click **Done**.

Starting workflow instances in bulk

As an administrator, you can start a single workflow that creates workflow instances in bulk. A workflow instance starts for each object that meets the start conditions.

Before you begin

Verify that email notifications for a bulk process are configured. For more information, see [“Customizing email notifications for GRC Workflow”](#) on page 548.

Plan when you run the bulk update. Depending on how many workflow instances are started, the bulk process can take a long time and may affect system performance for other users.

About this task

You can run a bulk process for one workflow at a time.

Procedure

1. Click  > **Solution Configuration > Workflows.**
2. From the Workflow List, select a single workflow with a check mark.
Start Workflow displays as one of the bulk update options.
3. Click **Start Workflow.**
A message provides an estimated count of the affected objects.
4. Click **Start Workflow.**
A workflow instance starts for each object of the workflow's object type if all of the following conditions are met:
 - The workflow is published.
 - The workflow is enabled.
 - An object is not locked.
 - An object is not currently in another workflow process.
 - An object meets the workflow's applicability criteria.
 - Your user is allowed to start a workflow for an object, given the conditions and applicability defined in the workflow. For all workflow instances that are started, your user is saved in the System Workflow Fields:Workflow Start User field.
5. When the process finishes, go to My Background Processes and review the log.
You receive an email that summarizes the bulk process. The assignees and subscribers of the workflow also receive email notifications.

Managing workflow instances

Monitor workflow instances to ensure that they are completing in a timely manner. Terminate stopped or blocked workflow instances.

Procedure

1. Click  > **Solution Configuration > Workflows.**
2. Click **Workflow Instances.**
A list of active workflow instances is displayed.
3. Filter the list of workflow instances by:
 - **Criticality**
 - **Workflow name**
 - **Stage**
 - **Type** (object type)
4. You can sort the list by fields in the header row.
5. You can click a workflow instance to open it.
6. To terminate a workflow instance, select it and click **Terminate Workflow Instances.**
The workflow instance is deleted. The object the workflow was based on remains but the workflow information, for example, workflow name, stage, and assignee, is removed. You can restart the workflow for the same object if needed.

Exporting and importing workflow definitions

You can migrate workflow definitions from one environment to another environment using Export Configuration and Import Configuration.

Before you begin

Read Chapter 26, “[Migrating OpenPages environments](#),” on page 865 to ensure that you are familiar with how to use Export Configuration and Import Configuration.

About this task

When you export workflows using Export Configuration, the workflow definitions you select are exported to a migration file. The email templates referenced in the exported workflow files are also automatically exported. Task Views and object types that are referenced in the workflows are not exported.

Procedure

1. Follow the instructions described in “[Exporting configuration items from the source environment \(Task Focused UI\)](#)” on page 873 and choose the workflows to export.
2. Follow the instructions described in “[Importing a migration file \(Task Focused UI\)](#)” on page 877 to import the migration file into a target environment.
3. Access and test the workflows in the target environment. Verify that the Task Views and object types work with the Task Views you migrated.

Customizing email notifications for GRC Workflow

You can customize the content of the email notifications that are generated by GRC Workflow by defining application text that is specific to your organization.

Before you begin

Learn about the **Email** setting on workflow actions. For information, see “[Defining a workflow action](#)” on page 527.

Learn about the **End Stage Notifications** setting on workflow end stages. For information, see “[Defining an end stage](#)” on page 523.

Learn about starting workflow instances in bulk. For information, see “[Starting workflow instances in bulk](#)” on page 546. At the end of a bulk update process, a summary email notification is sent to the administrator who started the process and email notifications are sent to assignees and subscribers.

Ensure that registry settings that apply to email notifications have been defined. For information, see “[Setting up GRC Workflow](#)” on page 495.

About this task

You can use the default email template as-is or customize the text to meet your requirements. There is one email template for all workflows and all object types. It is used for email notifications that are sent to users and summary email notifications that are sent to administrators who start a bulk update. The text and fields must be appropriate for broad use. You cannot create a new template.

If you operate in multiple locales, you can define email content in different languages. The template is designed for multiple formats, including tablets and phones.

If you customize the text, you define the content of the email notifications using application text strings. The email subject content is plain text. The email body content is formatted in HTML. You can apply styles using embedded style sheets.

You can also insert variables and fields in the email body content. For more information, see “[Using variables, functions, and fields](#)” on page 503. All the variables and fields that are listed there can be inserted in the email body content. Since there is only one email template for all workflows, insert system

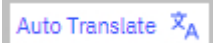
workflow fields rather than object fields. For more information, see [“System workflow fields” on page 502](#).

Example:

```
<!DOCTYPE HTML>
<html>
<head></head>
<body style="font-family: ibm-plex-sans,HelveticaNeue,Helvetica,Arial,sans-serif; font-size: 14px;">
<h1 style="font-size: 20px; font-weight: 300; padding: 22px 24px;">IBM <span style="font-weight: 600">OpenPages with Watson</span></h1>
<hr style="margin: 0; border-bottom: 2px solid #009e9a"/>
<div style="padding: 8px 24px 32px; background-color: #f3f3f3;">
<h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">[{$System Fields:Object Type Label$}]</h2>
<p style="margin: 0"><a href="[{$System Fields:Task View URL$}]">[{$System Fields:Name$}]</a></p>
<h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">[{$ApplicationText/app.workflow.workflowInfo.duedate.label$}]</h2>
<p style="margin: 0; display: none[{$DaysFromNow/System Workflow Fields:Stage Due Date$}]">Due in [{$DaysFromNow/System Workflow
Fields:Stage Due Date$}] days ([{$System Workflow Fields:Stage Due Date$}])</p>
<h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">[{$ApplicationText/app.workflow.workflowInfo.criticality.label$}]</h2>
<p style="margin: 0">[{$System Workflow Fields:Workflow Criticality$}]</p>
</div>
<div style="padding: 8px 24px 160px;">
<h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">[{$ObjectText/System Fields:Description$}]</h2>
<p style="margin: 0">[{$System Fields:Description$}]</p>
<h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">[{$ApplicationText/app.workflow.workflowInfo.stage.label$}]</h2>
<p style="margin: 0">[{$System Workflow Fields:Stage Name$}]</p>
<h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">[{$ApplicationText/app.workflow.transition.status$}]</h2>
<p style="margin: 0">[{$System Workflow Fields:Workflow Status$}]</p>
</div>
<hr style="margin: 0; border-bottom: 1px solid #767676"/>
<div style="padding: 32px 24px;">This email was automatically generated by [{$ApplicationText/product.name$}].</div>
</body>
</html>
```

Procedure

1. Click  > **System Configuration** > **Application Text**.
2. Click  to access the search filter.
3. Click **Email Templates**.
4. Use **Search** to further refine the list.
5. Select the application text you want to modify:
 - com.wf.email.template.default.assignee.subject contains the text in the subject line of emails sent to assignees.
 - com.wf.email.template.default.assignee.body contains the text in the body of emails sent to assignees.
 - com.wf.email.template.default.subscriber.subject contains the text in the subject line of emails sent to subscribers.
 - com.wf.email.template.default.subscriber.body contains the text in the body of emails sent to subscribers.
 - com.wf.email.template.default.action.complete.subject contains the text in the subject of emails for long running processes. This email informs the user that the process has finished. It is sent to the person who started the action.
 - com.wf.email.template.default.action.complete.body contains the text in the body of emails for long running processes. This email informs the user that the process has finished. It is sent to the person who started the action.
 - com.wf.email.template.bulk.start.subject contains the subject line of emails for Start Workflows bulk update (long running processes). This email informs the user that the process has finished. It is sent to the person who started the action.
 - com.wf.email.template.bulk.start.body contains the text in the body of emails for Start Workflows bulk update (long running processes). This email informs the user that the process has finished. It is sent to the person who started the action.
 - com.wf.email.template.bulk.start.failure.part contains the failure text in the body of emails Start Workflows bulk update (long running processes). This email informs the user about failures. It is sent to the person who started the action.
6. For each locale, enter the content that you want to appear in the email notification.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

7. Click **Done**.

Reporting on information in workflow instances

You can write reports that include information from workflow fields on workflow instances.

Before you begin

- Define the Include Workflow Fields setting as true. For more information, see [“Including workflow fields”](#) on page 958.
- Regenerate the reporting framework to make workflow instance data available to report authors.

About this task

All object types have workflow fields. Report authors can include those fields in reports. For more information, see [“System workflow fields”](#) on page 502.

The full set of information is available in both CQM and DQM Standard framework models, while a subset is available in Basic framework models. The information is available in workflow-specific query subjects and a subset of the information is available on every object type in the framework.

Chapter 16. Scheduler

Use the Scheduler to define and manage jobs that are run manually or on a schedule. The Scheduler is also used to view job executions that have completed.

Managing jobs

Use the Scheduler to manage jobs.

To access the Scheduler, click  > **Solution Configuration** > **Scheduler**. Whether the menu item is displayed depends on your access permissions.

Kinds of jobs

The Scheduler is used to manage the following kinds of jobs:

- Custom jobs

Custom jobs are user-defined jobs that perform a function. These jobs are configured, edited, viewed, manually started, and deleted in the Scheduler.

- JSP report jobs

A JSP report job is a custom job that runs a JSP report. These jobs are configured, edited, viewed, manually started, and deleted in the Scheduler.

For more information, see [“Defining a job that runs a JSP report” on page 554](#).

- Workflow Start jobs

Workflow Start jobs are created automatically in the Scheduler for workflows that are defined with a scheduled start. They can be viewed and manually started in the Scheduler. You can edit the description of the job but the schedule cannot be changed in the Scheduler. For more information, see [“Defining a workflow” on page 513](#).

- Ascent job

The Ascent job is displayed automatically in the Scheduler if the Ascent feed is used. The job defines the configuration and scheduling for the Ascent feed. You can view, edit, and start the job manually.

For more information, see [“Ascent Connector” on page 1039](#).

- Reg-Track job

This job is displayed automatically in the Scheduler when you run a Reg-Track import.

For more information, see [“Reg-Track Connector” on page 1049](#).

- SecurityScorecard job

The SecurityScorecard job is displayed automatically in the Scheduler if the SecurityScorecard feed is used. The job defines the configuration and scheduling for the SecurityScorecard feed. You can view, edit, and start the job manually.

For more information, see [“SecurityScorecard connector for IBM OpenPages Third Party Risk Management” on page 1071](#).

- SupplyWisdom job

The SupplyWisdom job is displayed automatically in the Scheduler if the SupplyWisdom feed is used. The job defines the configuration and scheduling for the SupplyWisdom feed. You can view, edit, and start the job manually.

For more information, see [“Supply Wisdom connector for IBM OpenPages Third Party Risk Management” on page 1073](#).

- Thomson Reuters Regulatory Intelligence job

This job is displayed automatically in the Scheduler when you run a Thomson Reuters Regulatory Intelligence import.

For more information, see [“Thomson Reuters Connector” on page 1041](#).

- Wolters Kluwer job

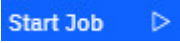
This job is displayed automatically in the Scheduler when you run a Wolters Kluwer import.

For more information, see [“Wolters Kluwer Connector” on page 1054](#).

Schedule List

When you click  > **Solution Configuration** > **Scheduler**, a Schedule List is displayed.

From the Schedule List, you can:

- Select the check box next to single or multiple jobs and click  to manually start a job. You might want to start a job manually if you do not want to wait for the next scheduled time or if the job has no schedule.

The Start Job Report window displays the number of jobs that started and failed.

- Click a job name. Information about the job opens in a new tab. Select the **Executions** tab to view information about each job execution.
- Click the **Job Name** column header to change the sort order of the list.
- Select the check box next to single or multiple jobs. The bulk update options are:
 - Enable
 - Disable
 - Delete
 - Start Job
- Click  to filter the Schedule List by category:
 - Ascent
 - Custom
 - Workflow Start

Create a new custom job

Click **Add New** to create a new job. For more information, see [“Defining a custom job” on page 553](#).

Delete a custom job

To delete a custom job, select a job from the Schedule List and click **Delete**. Non-custom jobs, for example, Workflow Start and Ascent jobs, cannot be deleted in the Scheduler.

Disable a job

To disable a job, select a job from the Schedule List. Select **Disable**.

Defining a custom job

A custom job definition contains information about a job and when it is executed.

Before you begin

Implement the Java class. For more information, see [“Implementing a Java class for custom jobs”](#) on page 556.

About this task

A custom job is typically defined with a schedule so that it runs, for example, every night at midnight. But a custom job can also be defined without a schedule. A custom job, like all jobs, can be started manually at any time.

Procedure

1. Click  > **Solution Configuration** > **Scheduler**.
2. Click **Add New**.
The **Add Job** panel opens.
3. Enter an internal **Name** for the custom job. It cannot be changed later.
Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
4. Enter a **Description**.
5. Enter a **Java class name** of the class that you created as a prerequisite.
6. Leave **Enabled** selected. It can be changed later.
7. In **Custom configuration** click **Add** to define properties that are name-value pairs needed by the Java class.
 - a) Enter a **Name**.
 - b) Set **Encrypt** to true or false.
 - c) Enter a **Value**.
8. Click **Edit** next to **Schedule** to set up a repeatable schedule. Otherwise, leave **Schedule** set to Not scheduled.
 - a) Enter a **Name**.
The **Name** displays in the Scheduler as the **Schedule Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
 - b) Enter a **Description** (optional).
 - c) Select a schedule type in **Define Schedule**:
 - Recurring
 - Specified Date/Time
 - Cron Expression
 - d) If you chose Recurring:
 - Select a value in **Repeat** (Daily, Weekly, Monthly, Quarterly) and add details such as day, month, or quarter.
 - Enter a **Time of Day**.
 - Select an **End Date** (optional).
 - e) If you chose Specified Date/Time:
 - Select a **Date**.
 - Enter a **Time of Day**.

f) If you chose Cron Expression:

- Enter a **Cron Expression**.
- Select an **End Date** (optional).

Advanced users can choose a cron expression if a Recurring or Specified Date/Time schedule does not meet your needs. Use the syntax for cron expressions, not crontab expressions.

g) Click **Done**.

9. Click **Done**.

Defining a job that runs a JSP report

You can use the Scheduler to create jobs that automatically run JSP reports.

Before you begin

- To do this task, you need the **Scheduler** application permission.
- You need a JSP report. For more information, see [“Creating an interactive JSP report \(Task Focused UI\)” on page 181](#).

About this task

You run JSP report jobs by using a custom job, which is available by default. You specify the JSP report to run, parameters for the job, and when to run the job.

For example, you can create a job that runs the KRI Creation Utility each week. The KRI Creation Utility is a JSP report that identifies KRIs that require values and sends notification emails to the KRI owners. Each week, the job runs the utility and sends the notifications automatically.

If the JSP report takes parameters, such as the name of a business entity or a profile, you can pass those parameters to the job.

The following table shows the required and optional parameters for JSP report jobs.

Item	Description
Java class	<code>com.ibm.openpages.api.service.local.scheduler.jobs.JSPReportJob</code>
Required parameter	JSPReport – Specifies the path to the JSP report. For example: Reporting/Hidden Reports/ORM Custom Reports/KRI Creation Utility/KRI Creation Utility
Optional parameters	• OutputEntity – Specifies the full path to a Business Entity object. The report output is attached to the Business Entity that you specify. • SaveOutput (true false) -- Specifies whether the output of the report is saved. Default is false. If SaveOutput is true and OutputEntity is empty, the report output is saved to the /aurora/output/jspreport directory on the application server. • Report parameters – If the JSP report uses parameters, you can add the parameters to the job definition. Parameter names must match the report parameter names exactly. If you add a parameter to the job definition, you must provide a value for the parameter. You cannot leave a parameter value empty.

Item	Description
	If the value of a parameter contains spaces, surround the value with quotation marks.

Procedure

- Log on to the Task Focused UI as an administrator.
- Collect the information that you need to run the JSP report:
 - Click  > **System Configuration** > **Pages and Templates**, locate the JSP report, and then click its name.
The report's details are displayed.
 - Get the report name and folder:
Copy the text in the **Folder** field. Remove / _cw_channels /, and then remove the spaces between each /. Add the report's name to the path.
For example: Reporting/Hidden Reports/ORM Custom Reports/KPI Creation Utility/KPI Creation Utility
 - If the JSP report uses parameters, get the parameter names. The parameter names are shown in the **Page Details** section.
 - If you want to attach the report output to a business entity, get the business entity's full path:
Click **Organization** > **Business Entities**, click the name of the business entity you want to use, and copy the value of the **Folder** field.
- Click  > **Solution Configuration** > **Scheduler**.
- Click **New Job**.
The **New Job** panel opens.
- Enter a **Name** for the job. You can't change the name later.
Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
- Enter a **Description**.
- In the **Java class name** field, paste the following text:


```
com.ibm.openpages.api.service.local.scheduler.jobs.JSPReportJob
```
- Leave **Enabled** selected. You can change it later.
- In **Custom configuration** click **New**.
- In the **Name** field, type JSPReport. In the **Value** field, type the path the JSP report.
- To define other parameters, click **New** and enter the parameter's name and value. Repeat this step for each parameter that you want to add.
- Optional: To set up a repeatable schedule for the job, click **Edit** next to **Schedule** Otherwise, leave **Schedule** set to Not scheduled, and go to step 13.
 - Enter a **Name**.
The **Name** displays in the Scheduler as the **Schedule Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
 - Enter a **Description** (optional).
 - Select a schedule type in **Define Schedule**:
 - Recurring
 - Specified Date/Time
 - Cron Expression

d) If you chose **Recurring**:

- Select a value in **Repeat** (Daily, Weekly, Monthly, Quarterly) and add details such as day, month, or quarter.
- Enter a **Time of Day**.
- Select an **End Date** (optional).

e) If you chose **Specified Date/Time**:

- Select a **Date**.
- Enter a **Time of Day**.

f) If you chose **Cron Expression**:

- Enter a **Cron Expression**.
- Select an **End Date** (optional).

Advanced users can choose a cron expression if a Recurring or Specified Date/Time schedule does not meet your needs. Use the syntax for cron expressions, not crontab expressions.

g) Click **Done**.

13. Click **Create**.

Implementing a Java class for custom jobs

A custom job is a user-defined job that performs a function. It is implemented as a Java class that can be executed manually or on a schedule.

Custom jobs must be deployed to each OpenPages application server and are dynamically loaded during startup.

To implement a custom job, complete the following tasks:

- Create a custom job Java class by extending the following abstract implementation:

```
com.ibm.openpages.api.scheduler.AbstractScheduledProcess
```

- Add the class to a JAR file. Use the JAR file for all of your custom code. Deploy the JAR file to each OpenPages application server in the `<OP_HOME>/aurora/op-ext-lib` directory.
- Restart the OpenPages application servers so that the custom job can be picked up by the dynamic class loader.
- Use the Scheduler to add a custom job that uses the Java class. Set any property values or fields that the custom job requires as inputs. For more information, see [“Defining a custom job” on page 553](#).

Providing configuration information to a custom job

For a custom job to be useful, it might require configuration information. For example, if it needs to connect to another service, it may need to know the API key. These values are defined as configuration items in the custom job in the Scheduler and passed into the custom job at run time.

Configuration items are string name-value pairs that you define.

The custom job needs to validate that the properties that it expects to be passed in have been passed in and that they have valid values.

Authoring the custom job Java class

The only requirement of a custom job Java class is that it extends `com.ibm.openpages.api.scheduler.AbstractScheduledProcess`. This requirement is validated when the custom job is defined in the Scheduler.

A single abstract API from `AbstractScheduledProcess` called `execute` must be implemented in your derived Java class, as follows:

```
void execute(){  
    //add your custom code here  
}
```

Within this method is where you write the functionality that the custom job performs.

To access the configuration values, call:

```
this.jobDetail.getJobConfiguration();
```

For more information about the OpenPages GRC API, which you can use in custom jobs, see the *IBM OpenPages with Watson API Javadoc*. For links to the Javadoc, see [Appendix G, “OpenPages API documentation,” on page 1121](#).

Exception or validation messages can be thrown from a custom job and displayed to the user. To display messages, use:

```
throwException(String message, Throwable cause)
```

Use this method to throw exceptions and display a custom message to users. Uncaught exceptions or exceptions that are explicitly thrown are logged by the application, but only a general error message is displayed to users.

Chapter 17. Localizing text

You can localize display text for object types and fields, and for a variety of application objects and custom return values. You can manage localized text that displays to users for predefined object types, object fields that are supplied by IBM OpenPages with Watson or that you create, and application objects.

Locale codes

The OpenPages with Watson application provides translation support in several languages for predefined object text. Each supported language has a corresponding locale code that is listed under the object text. The locale code consists of a language code (for example, "fr" for French) and a country or region code (for example, "FR" for France).

The following table lists the supported languages with their corresponding locale code.

Table 186. Supported Languages and Locale Codes	
Language	Locale Code
German	de_DE
U.S. English	en_US
U.K. English	en_GB
Spanish	es_ES
French	fr_FR
Italian	it_IT
Japanese	ja_JP
Brazilian Portuguese	pt_BR
Simplified Chinese	zh_CN
Traditional Chinese	zh_TW
Report Design Language	en_CA
Note: Users authoring reports in the reporting tool must select this language prior to creating or modifying reports.	

The default language for object text that has not been translated is U.S. English.

You can globally set a default language in which the application user interface is displayed to users and optionally enable auditing of translation label changes. For details see [“Set localization options” on page 639](#).

Configuring client systems to display Asian characters

You can install language packs on Microsoft Windows client machines to see Windows in other languages.

Note: For users who use the Japanese locale, client machines must have the Windows Japanese language pack installed. If this pack is not installed, IBM OpenPages with Watson users will notice that the browser title bar and some pop-up messages contain unreadable characters.

For more information, see [Language packs for Windows](#).

Language and locale support

If you are using IBM OpenPages with Watson in a language other than English, this information will help you to understand the language and locale settings.

Web browser language preference

The web browser language preference is the setting that you choose to specify the language that web pages can be displayed in. The web browser language preference affects only the OpenPages with Watson login page. The web browser language preference does not affect number and date formatting in OpenPages with Watson.

If the web browser language preference is set to a language other than one of the following languages, be aware that the OpenPages with Watson login page appears in English:

- German
- Spanish
- French
- Italian
- Japanese
- Portuguese
- Chinese
- English

Locale setting

The **Locale** list contains a list of product languages. This language setting controls the language of the product except for the login page.

Data formatting and report languages are available in the following cultures in the **Locale** list:

Table 187. Languages in the Locale list and the cultures that they represent	
Language in the Locale list	Culture
French	French (France)
German	German (Germany)
Italian	Italian (Italy)
Japanese	Japanese (Japan)
Portuguese	Portuguese (Brazil)
Spanish	Spanish (Spain)
Simplified Chinese	Chinese (China)
Traditional Chinese	Chinese (Taiwan)
U.K. English	English (UK)
U.S. English	English (US)

Considerations for specific languages

When OpenPages with Watson is set to use U.S. English, dates are formatted as mm/dd/yy. For example, January 3, 2020, is formatted as 1/3/20 rather than 03/01/2020 in U.K. English.

When the product is set to use Spanish (Spain), numbers are formatted as 123.456,78, where the period is a thousands separator and the comma is used as a decimal separator. For example, the number twelve

thousand and five hundred is formatted as 12.500 in Spanish (Spain) rather than 12,500 in Spanish (Mexico).

In several cultures, the convention is to place the currency symbol after the number. In OpenPages with Watson, currency symbols are always displayed before the number.

Date formatting can be unconventional as well.

Localizing object text

Object text is the descriptive label name that displays in the application for object types, object fields, filters, and enumerated values. You can translate and modify object text for a specific locale.

For a list of supported locales, see the topic, [Chapter 17, “Localizing text,” on page 559](#).

Object text can be defined in either the Task Focused UI or the Standard UI. Changes made in one interface are immediately reflected in the other. For more information, see:

- [“Modifying object text \(Task Focused UI\)” on page 561](#)
- [“Modifying display text for an object text \(Standard UI\)” on page 563](#)

You can modify the following object text for a locale:

- The singular and plural labels that display the name of an object type (for example, "Risk" and "Risks" for the Risk object type) or custom form (such as a survey) wherever that object type appears in the application. For more information, [“Modifying object text \(Task Focused UI\)” on page 561](#).
- A singular label that displays:
 - The name of an object field in an object view.
For example, if you had an object field called "Impact" that displayed the label text "Impact", you could change the label text to display "Severity of impact" instead.
 - The value or values of an enumerated object string that are displayed on an object's details page.

Note:

- Only plain text should be entered as object text in labels. Light formatting is supported for field guidance text strings. HTML and line breaks are not supported.
- Object text has a 4000 character maximum per label.

Object text is grouped primarily by object type with an additional group for unassigned field groups.

For example, the SOXControl group contains the label text for the Control object and its related field groups.

The Unassigned Field Groups group contains the label text for field groups that are either not assigned to an object type or are commonly used by all object types, such as System Fields, Currency Attributes, Publishing, and so forth.

Important: Do not change or translate currency codes.

Modifying object text (Task Focused UI)

You can modify object text strings for object types, object fields, filters, and enumerated values.

About this task

To do this task, you need the **SOX > Administration > Object Text** application permission.

You can use the **Manage Object Text** task in the Task Focused UI to modify all object text strings, not just those that appear in the Task Focused UI.

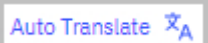
The **Category** column on the **Object Text** page describes what type of text the object type contains.

Table 188. Using the Category column

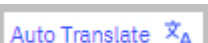
If the Category column is...	The object text defines ...
Enum Value	Label text for an enumerated value for an object field
Field	Label text and field guidance for an object field
Filter	Label text for a public filter
Object	Singular and plural forms of the displayed label text for an object type or custom form object type

Procedure

- Click  > **System Configuration** > **Object Text**.
- To find object text that you want to view or modify, click  to access the search filter.
 - Select one or more object types in **Object Type**.
 - Select one or more filters in **Search Scope**.
 - Optional: Click in the Search box and enter free text. The search returns results when it finds a match in the item, description, or labels in any language. You can enter single words. For example, enter "audit" to find all object texts with the word "audit" in the item, description, or labels. The Search box text is not case-sensitive.
- To modify labels for an enumerated value for an object field:
 - Click the row for the enumerated value object text that you want to update (the **Category** column is **Enum Value**).
 - For selected locales, enter text in **Label**.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).
 - Click **Done**.
- To modify labels and guidance for an object field:
 - Click the row for the object field text that you want to update (the **Category** column is **Field**).
 - For selected locales, enter text in **Label** and **Guidance**.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).
 - Optional: Apply formatting in **Guidance**. For more information, see [“Applying light formatting to text” on page 403](#).
 - Click **Done**.
- To modify labels for a filter:
 - Click the row for the filter that you want to update (the **Category** column is **Filter**).
 - For selected locales, enter text in **Label**.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).
 - Click **Done**.
- To modify labels for an object type:
 - Click the row for the object type that you want to update (the **Category** column is **Object**).
 - For selected locales, enter text in **Singular Label** and **Plural Label**.



If it is displayed, click [Auto Translate](#) to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 1018](#).

IBM Watson Language Translator can correctly translate singular and plural text.

c) Click **Done**.

Modifying display text for an object text (Standard UI)

You can modify the value for the singular and plural forms of the displayed label text for any object type or custom form object type (such as a survey). These labels appear in the IBM OpenPages with Watson application interface wherever the particular object type displays, such as on a menu (for object types) or in object views.

Tip: You can define object text in the Task Focused UI. For more information, see [“Modifying object text \(Task Focused UI\)” on page 561](#).

Procedure

1. Click **Administration > Object Text**.
2. On the **Object Text** page, click the name of the object type you want to modify (for example, SOXRisk).
3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US).
4. On the **Locale Code** detail page, make the required changes in the **Singular Label** box and **Plural Label** box to the display label text as needed.
5. Click **Save**.

Modifying display text for object fields (Standard UI)

You can modify the value of the displayed label text for any object field, including field guidance. These labels appear in the IBM OpenPages with Watson application interface wherever the particular object type displays in an object view, such as a detail or folder view page.

If the object field is an enumerated string data type, each string value is also displayed and can be modified as needed.

Procedure

1. Click **Administration > Object Text**.
2. On the **Object Text** page, expand the object type you want, expand the field group you want, and click the name of the object field that you want to modify. To modify enumerated string values, on the **Object Text** page, expand the enumerated object field you want, and click the name of the value that you want to modify.
3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US).
4. On the **Locale Code** detail page, make the required changes.
5. Click **Save**.

Modifying display text for public filters (Standard UI)

You can modify the value of the displayed label text for public filters. In a Filtered List View, the label text for filters is typically displayed under "Public filters" in the filters list.

Procedure

1. Click **Administration > Object Text**.

2. On the **Object Text** page, expand the object type you want, expand the filters (🔍 icon), and click the name of the filter that you want to modify.
3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US).
4. On the **Locale Code** detail page, make the required changes:
5. Click **Save**.

Localizing system fields

You can change the system fields used for unassigned field groups that are specific to a locale. This change affects all object types and views.

For a list of supported locales, see [Chapter 17, “Localizing text,” on page 559](#).

Procedure

1. Click  > **System Configuration** > **Object Text**.
2. Click  to access the search filter.
3. Click **Unassigned Field Groups** in **Object Type**.
4. Click **System Fields** in **Search Scope**.
5. Select the name of the field that you want to change.
6. Click the name of the locale code you want to change, for example, en_US.
7. Make the required changes.
8. Click **Done**.

Localizing application text

Application text is the descriptive label names for core parts of the system.

Application text is static, which means that it is unlikely to change over time. You can modify application text that is specific to a locale. For list of supported locales, see [Chapter 17, “Localizing text,” on page 559](#).

Application text applies to core parts of the system while object text applies to text strings that are specific to object types, for example, object names, fields names, and so on. For more information about object text, see [“Localizing object text” on page 561](#).

Application text can be defined in either the Standard UI or the Task Focused UI. Changes made in one interface are immediately reflected in the other. For more information, see:

- [“Modifying application text \(Task Focused UI\)” on page 566](#)
- [“Modifying application text \(Standard UI\)” on page 567](#)

You can modify locale-specific application text for:

- The text label that displays for an application text.
- The format for the display of names and numeric data. For examples, see [“Modifying the bucket heading format of the phonebook” on page 567](#) and [“Modifying the user name format” on page 568](#).

Note: Application label text is limited to 4000 characters. Application text names and descriptions are limited to 256 and 2048 characters, respectively.

The following table shows the groupings by folder category for application text:

Table 189. Application text folder categories

This folder	Contains the label text for
Application Messages	Messages that are displayed for dependent fields and pick lists, and System Admin Mode.
Buttons	The icons that are used within the application. For example, <code>com.button.back</code> contains the text for the Back icon, <code>button.copy</code> contains the text for the Copy icon.
Column Headings	The table column headings that is used in the object views throughout the application and in JSP Notification Manager reports. For example, <code>com.column.heading.start.date</code> contains the text for the Start Date column, <code>jspreports.notification.tests.column.parent</code> contains the text for the Parent column in the JSP Notification report.
Custom	User-defined keys. For more information, see “Creating a custom setting” on page 634 .
Email Templates	Text strings that are part of email notifications.
Exceptions	Messages that are displayed to users when an error condition occurs. For example, <code>com.exception.object.profile.not.found</code> contains the text for the error message displayed when a profile is not found, <code>exception.file.delete</code> contains the text for the error message displayed when a user does not have permission to delete a file.
Formats	The formatting of numeric and name display text. For details, see “Modifying application text (Task Focused UI)” on page 566 .
Labels	Objects that are not considered objects, such as administrative tasks, and configuration objects. For example, <code>com.label.acl.read</code> contains the text for the Read property on the Access Control details page, <code>com.label.email</code> contains the text displayed next to the email input box on the User create and edit pages.
Menu Items	Links to all other menu items that are not listed on the menu bar. For example, <code>com.menu.item.admin.object.profile</code> contains the text for the Profile link on the Administration menu, <code>com.menu.item.admin.reporting.schema</code> contains the text for the Reporting Schema link on the Administration menu.
Miscellaneous	A variety of objects that do not belong to other groups. Includes label text for such objects as guided action, page footer, reporting status, notification messages, and so forth.
Reporting Framework	Objects that are used by the Reporting Framework.
Table Headings	Messages that are displayed to users within a table as well as the tabs (tabular headings for a table). For example, <code>com.table.empty.users</code> contains the text that displays in the User listing table when no users are found, <code>com.table.heading.object.field</code> contains the text for the Object Field Information tab on the Object Field details page.
Titles	The initial portion of the breadcrumb trail.

Table 189. Application text folder categories (continued)

This folder	Contains the label text for
Validation Messages	Messages that are displayed to users when invalid information has been entered in a field or to confirm a specific user action such as entering or exiting System Admin Mode or deleting any objects. For example, <code>com.validation.logon.username.required</code> contains the message text displayed when a user name is missing such as when it is created or when a user logs on, <code>file.delete.confirmText</code> contains the text in the confirmation prompt window that displays during a delete operation.

Modifying application text (Task Focused UI)

You can modify the value of the displayed label or text for any application object (such as icons, labels, report names and descriptions, messages). The process for modifying display text is the same for all application objects, including reports.

About this task

To do this task, you need the **SOX > Administration > Application Text** application text.

You can use the Task Focused UI to modify all application text strings, not just those that appear in the Task Focused UI.

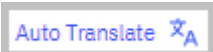
Changes to the displayed text appear wherever the particular object is displayed in the application.

Procedure

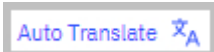
1. Click  > **System Configuration > Application Text**.
2. To find application text that you want to view or modify, click  to access the search filter.
 - a) Select one or more categories in **Search Scope**.
 - b) Optional: Click in the Search box and enter free text. The search returns a results when it finds a match in the name, description, or values in any language. You can enter single words. For example, enter "path" to find all application texts with the word "path" in the name, description, or values. The Search box text is not case sensitive.
 - c) Locate the application text that you want to modify.
3. To modify application text, click on an application text in the list. Make your changes in one or more locales.

If it is displayed, click  to populate translated values to languages. For more information, see ["IBM Watson Language Translator" on page 1018](#).

4. Click **Done**.
5. To add new application text, click **Add New**.
 - a) Enter a **Name**.
Allowed characters are A-Z, a-z, 0-9, period, underscore, hyphen, and spaces. Special characters are not allowed.
 - b) Select a **Category**.
 - c) Enter a **Description**.
 - d) Enter a **Default Label**.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator”](#) on page 1018.

- e) In the locale code that you want to modify, for example, French or Japanese, enter text for that language.

If you neither click  nor enter text for each locale code, the text in **Default Label** is populated to all languages.

- f) Click **Done**.

Modifying application text (Standard UI)

You can modify the value of the displayed label or text for any application object (such as icons, labels, report names and descriptions, messages). The process for modifying display text is the same for all application objects, including reports.

Changes to the displayed text appear wherever the particular object is displayed in the application.

Tip: You can define application text in the Task Focused UI. For more information, see [“Modifying application text \(Task Focused UI\)”](#) on page 566.

Note:

- The Miscellaneous folder typically contains a listing of report name and description keys for localizing the display text of reports that were automatically published by the system. For information about automatically publishing Cognos reports, see [“Adding reports to OpenPages with Watson”](#) on page 171.
- For reports that are manually published and require localized display text on the application user interface for multiple languages, keys will need to be added to the Custom folder (see [“The Custom folder”](#) on page 576).

Procedure

1. Click **Administration > Application Text**.
2. On the **Application Text** page, open the folder that contains the label of the object field you want to modify (for example, Buttons or Miscellaneous), expand the folder, and click the name of the object field or key you want to modify.
3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US or ja_JP).
4. On the **Locale Code** details page, make the required changes in the **Label** box to the display label text as needed.
5. Click **Save**.

Modifying the bucket heading format of the phonebook

You can modify the format of the bucket heading in the phonebook style pop-up box of the User selector for a locale.

Note: You can also modify the bucket size of the phonebook. For more information, see [“Actor selectors: Configure the bucket size of the phonebook”](#) on page 605.

Procedure

1. Click  > **System Configuration > Application Text**.
2. Click  to access the search filter.
3. Click **Formats**.

4. Click the **com.user.bucket.name.format** application text.
5. Click the name of the locale code you want to modify, for example, en_US.
6. Modify the format. The default format is {0} - {1}.

The format string uses Java code. Generally, the {0} in the format string is a variable that is replaced by the name of the target object.

7. Click **Done**.

Example

To display a bucket heading with the name of the first person in the bucket followed by a dash and then the name of the last person in that bucket, you would enter the following codes in the Label field: {0} - {1}.

Modifying the user name format

You can control how user names are displayed for a locale. The default is first name, last name, email (%FN; %LN; - %EM).

When you change the display name format, the change occurs throughout the application wherever the person's name displays. For example, if you modified the name format so that the last name of the person was followed by the person's first name, that modified name format displays in the menu bar, user selector, and search result boxes.

Note: If an invalid format string is defined, only the user name will be displayed.

Procedure

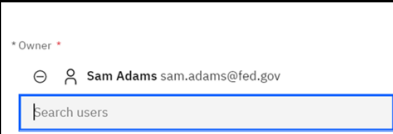
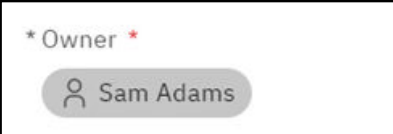
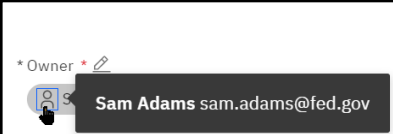
1. Click  > **System Configuration** > **Application Text**.
2. Click  to access the search filter.
3. Click **Formats**.
4. Click the **com.display.name.format** application text.
5. Click the name of the locale code you want to modify, for example, **en_US**.
6. Modify the format as follows:

To display this name format...	Type this code...	
User name	%NM;	Displays the value in the User Name field on the User Information page.
First Name	%FN;	Displays the value in the First name field on the User Information page.
Last Name	%LN;	Displays the value in the Last name field on the User Information page.
Email	%EM;	Displays the email address of a user in the Email object field on a User Information page.

In the Task Focused UI, combinations and special characters are allowed, except for the hyphen (-) character.

- For a field that is in an editable state, a hyphen applies bold formatting to the text in front of the hyphen.
- For a field that is in a read-only state, a hyphen shortens the display name. Only the text before the hyphen is displayed. The full display name is displayed in a tooltip when a user clicks the user icon.
- The hyphen character is not displayed in the user interface.

The following table shows a field in an editable state, a read-only state, and in a read-only state with the tooltip displayed. This example uses the %FN; %LN; - %EM; display format:

Editable state	Read-only state	Tooltip
		

In the Standard UI, the hyphen does not control formatting and it is displayed in the user interface.

7. Click **Done**.

Example

Assume that a user is defined where **User Name** is "jsmith", **First Name** is "Jane", and **Last Name** is "Smith".

Table 190. User name formatting in the Task Focused UI	
If com.display.name.format is set to ...	The user displays as ...
%NM;	jsmith
%FN;	Jane
%LN;	Smith
%FN; %LN;	Jane Smith
%FN; %LN; - %EM;	Jane Smith jsmith@co.com Or, if the field is in a read-only state: Jane Smith
%FN; %LN; - %NM;	Jane Smith jsmith Or, if the field is in a read-only state: Jane Smith
%FN; %LN; (%NM;)	Jane Smith (jsmith)
%FN; %LN; [%NM;]	Jane Smith [jsmith]
%NM; - %FN; %LN;	jsmith Jane Smith Or, if the field is in a read-only state: jsmith

Table 191. User name formatting in the Standard UI	
If com.display.name.format is set to ...	The user displays as ...
%NM;	jsmith
%FN;	Jane
%LN;	Smith
%FN; %LN;	Jane Smith
%FN; %LN; - %EM;	Jane Smith - jsmith@co.com
%FN; %LN; - %NM;	Jane Smith - jsmith
%FN; %LN; (%NM;)	Jane Smith (jsmith)
%FN; %LN; [%NM;]	Jane Smith [jsmith]

Table 191. User name formatting in the Standard UI (continued)	
If com.display.name.format is set to ...	The user displays as ...
%NM; - %FN; %LN;	jsmith - Jane Smith

Modifying overview menu links

You can globally modify the format of overview navigational links on menus.

By default, the format for overview links is {0} Overview where {0} represents the singular label of the object.

This format displays, for example, menu item links such as Risk Assessment Overview or Business Entity Overview.

Under the various menu headings on the menu bar, overview menu item links are typically listed before the other object view links. With the exception of Overview object links and the Business Entities link (which is a List view), all other object types have Filtered List View and/or Folder object views.

Procedure

1. Click  > **System Configuration > Application Text**.
2. Click  to access the search filter.
3. Click **Formats**.
4. Click the **menu.item.documentation.object.overview** application text.
5. Click the name of the locale code you want to modify, for example, en_US.
6. Modify the text. The singular label of the object type is represented by {0} in the format string.
7. Click **Done**.

To view the changes in the browser, users must log out and then log back in to the application.

Example

If you wanted to change the Overview link format from the singular object name followed by the text "Overview" (as in Risk Assessment Overview or Business Entity Overview) to "Overview" followed by the object name (as in Overview Risk Assessment or Overview Business Entity) you would enter the value in the Label box as:

Overview {0}

Modifying navigational view links

You can globally modify the format of Folder View or Filtered List View navigational links on menus.

By default, the format for these links is:

{0}

where {0} represents the plural label of the object.

This format displays, for example, menu item links such as Risks or Business Entities.

Procedure

1. Click  > **System Configuration > Application Text**.
2. Click  to access the search filter.
3. Click **Formats**.
4. Click the **menu.item.documentation.object.folder.view** application text.

5. Click the name of the locale code you want to modify, for example, en_US.
6. Add or edit text.

Note: The plural label of the object type (such as, Risks, Controls, Processes) is represented by {0} in the format string.

7. Click **Done**.

Example

If you wanted to change the Folder View or Filtered List View link format from the object type name (such as Risks or Controls) which is represented by {0}, to display the object type name followed by the text "View" (such as Risks View or Controls View), you would enter the value in the Label box as {0} View.

Defining messages and behavior on the login screens

You can define messages that are displayed on the login screen for OpenPages and configure certain behavior.

About this task

The login screen can contain the following messages:

- A system notice

Can be any text, for example, OpenPages will be unavailable on Sunday 8:00-14:00 due to system maintenance.

- Checkbox text

Can be any text, for example, I have read the privacy statement and I agree to the terms and conditions. The user must click the checkbox to log in.

- A privacy statement

Can be any text, for example, a company-wide statement about terms and conditions or privacy.

- A privacy statement link

Contains a link, for example, to an intranet site with more information about privacy. The link opens in a new tab.

The link is also used by the **Privacy** menu item in the Help menu in the Task Focused UI and the Standard UI.

- An acceptable use policy link

Contains a link, for example, to an intranet site with more information about acceptable use. The link opens in a new tab.

The link is also used by the **Acceptable Use** menu item in the Help menu in the Task Focused UI and the Standard UI.

You define a message's content by using application text strings. If a string is empty, the message is not displayed.

The following example shows all the messages. The numbers correspond to the application text strings listed in [Table 192 on page 572](#).

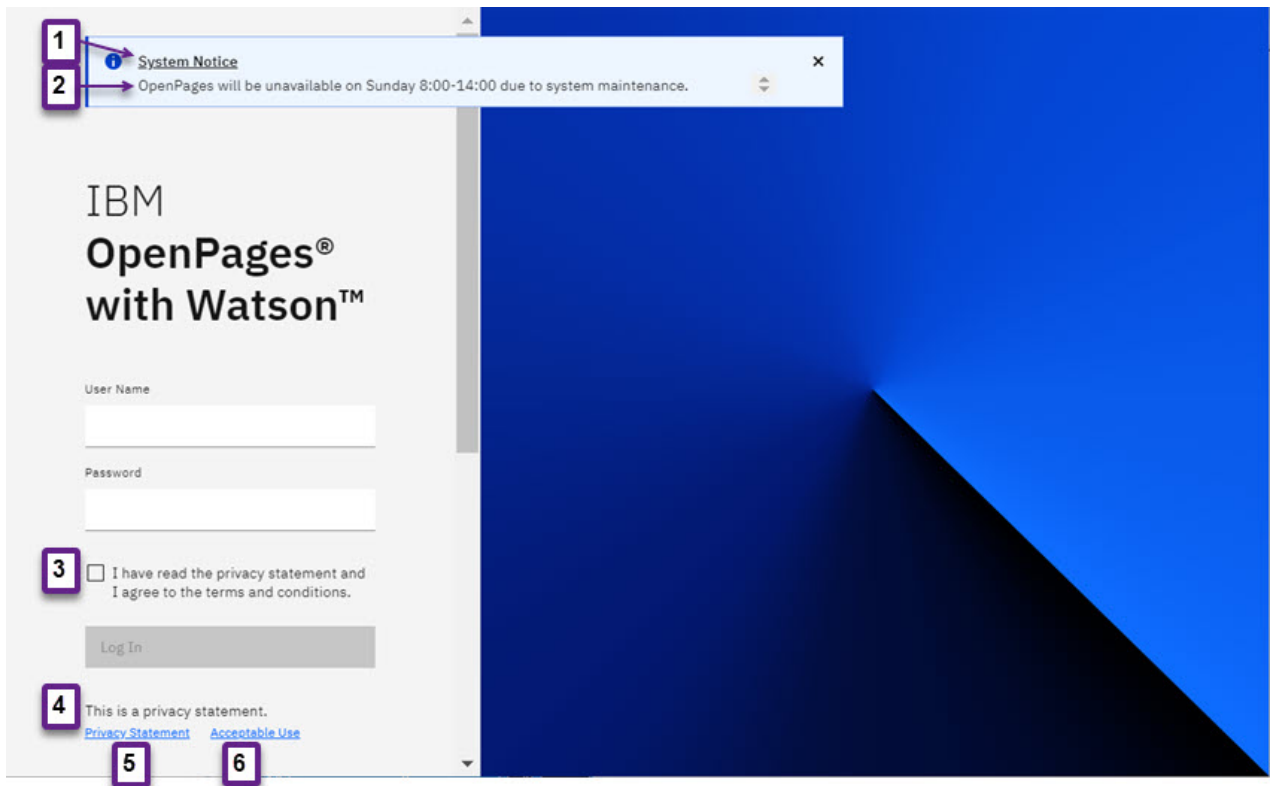


Figure 56. Login screen messages and application text strings

Table 192. Messages and application text strings		
#	Description	Located in the Application Text > Labels category
1	Title for a system notice. The default is System Notice.	com.label.logon.system.notice.header
2	Text for a system notice. If empty, the system notice box, including the system notice header, is not displayed. Default is empty.	com.label.logon.system.notice.text
3	Text displayed next to the checkbox. If empty, the checkbox and corresponding text is not displayed. Default is empty.	com.label.logon.checkbox.text
4	Text for a privacy statement. Default is empty.	com.label.logon.privacy.text
5	Title for a privacy statement link. Default is Privacy Statement. The link is displayed if a URL is defined in the Privacy Link URL registry setting.	com.label.logon.privacy.link
6	Title for an acceptable use policy link. Default is Acceptable Use. The link is displayed if a URL is defined in the Acceptable Use Link URL registry setting.	com.label.logon.acceptable.use

The placement of the messages on the login screen is fixed and cannot be changed.

Figure 56 on page 572 is the login screen for the Task Focused UI and the Standard UI.

Each locale can have one message. The user's locale determines the message that is displayed. The message that is defined in the en_US locale is the default message if the user's locale is not saved in the browser.

Note: The messages are displayed before users log in to OpenPages. Ensure that the content of the messages is appropriate for users who might not have access to OpenPages.

If you are using single sign-on (SSO), the login screen is bypassed. Users still see the messages, however.

- If only a system notice is defined, the system notice is displayed on the dashboard when users access the system. The system notice is displayed once per session. Changes are not immediately broadcast. The system notice header that is defined in **com.label.logon.system.notice.header** is not displayed on the dashboard.
- Otherwise, the messages are displayed on a blank page in OpenPages with a **Continue** button. If you defined checkbox text, users must click the checkbox to enable the **Continue** button. When users click **Continue**, they can access OpenPages.

For example, if you define a system notice and checkmark text, users see a page that is similar to the following page:

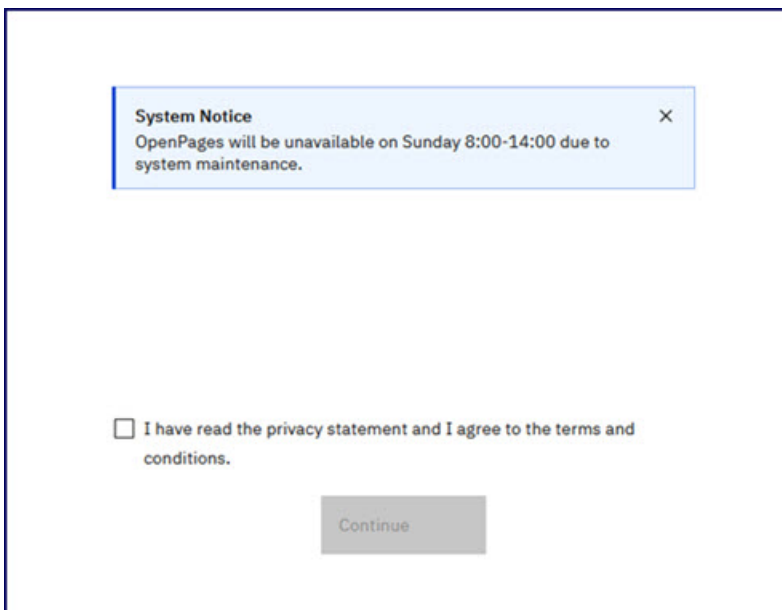


Figure 57. A system notice and check mark text displayed for SSO users

You can optionally add HTML formatting when you define application text strings, for example:

- `<b>text</b>` displays text in bold.
- `<br>` begins a new line.
- `<ul><li>List item 1</li><li>List item 2</li></ul>` inserts a bulleted list.
- `<a href="https://insert URL/" target="_blank">insert URL title</a>` inserts a link.

Procedure

1. Click  > **System Configuration** > **Application Text**.
2. Click  to access the search filter.
3. Click **Labels**.
4. Search for one of the following labels. Click the link to edit the application text.
 - **com.label.logon.system.notice.header**
 - **com.label.logon.system.notice.text**

- **com.label.logon.checkbox.text**
- **com.label.logon.privacy.text**
- **com.label.logon.privacy.link**
- **com.label.logon.acceptable.use**

5. Click the name of the locale code you want to modify, for example, **en_US**.
6. Add or edit message text.
7. Click **Done**.
8. If you defined a privacy statement link, specify the URL to display when users click the link.
 - a) Click  > **System Configuration** > **Settings**.
 - b) Edit the **Applications** > **Common** > **Privacy Link URL** setting. Specify the URL of the privacy statement.
9. If you defined an acceptable use policy link, specify the URL to display when users click the link.
 - a) Click  > **System Configuration** > **Settings**.
 - b) Edit the **Applications** > **Common** > **Acceptable Use URL** setting. Specify the URL of the acceptable use policy.

What to do next

Log on to OpenPages and verify that the messages display.

Tip: To remove a message, repeat the steps and clear the text in the **Label** box. If you added a privacy statement link or an acceptable use policy link, clear the value of its registry setting.

Defining the Privacy and Acceptable Use menu items

You can modify the **Help** menu in the Task Focused UI to include links to a privacy statement and an acceptable use policy. The menu items are also displayed on the Help menu in the Standard UI.

About this task

You can add the following items to the **Help** menu:

- A privacy statement menu item

Opens a link, for example, to an intranet site with more information about privacy. The link opens in a new tab.

The menu item is also displayed in the **Help** menu in the Standard UI.
- An acceptable use policy menu item

Opens a link, for example, to an intranet site with more information about acceptable use. The link opens in a new tab.

The menu item is also displayed in the **Help** menu in the Standard UI.

You define a menu item by using application text labels and registry settings.

Privacy Statement menu item

You define the menu item name in **app.header.privacy.label**. This name is what users see in the menu. The default is **Privacy Statement**.

You define the link in the **Applications** > **Common** > **Privacy Link URL** setting. When users click the menu item, this link opens in a new tab.

Note: This link is also used by the privacy statement link on the login page. For more information, see [“Defining messages and behavior on the login screens” on page 571](#).

Acceptable Use Policy menu item

You define the menu item text in **app.header.acceptable.use.label**. This name is what users see in the menu. The default is **Acceptable Use Policy**.

You define the link in the **Applications > Common > Acceptable Use URL** setting. When users click the menu item, this link opens in a new tab.

Note: This link is also used by the acceptable use policy link on the login page. For more information, see [“Defining messages and behavior on the login screens”](#) on page 571.

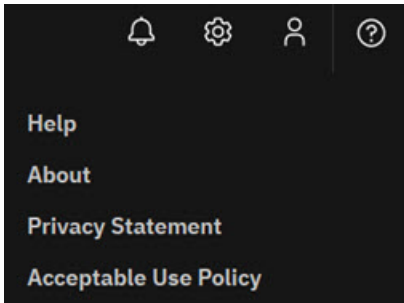


Figure 58. Help menu with the Privacy and Acceptable Use menu items

The placement of the **Privacy Statement** and **Acceptable Use Policy** items in the menu is fixed and cannot be changed.

Each locale can have one name for a menu item. The user's locale determines the text that is displayed. The text that is defined in the en_US locale is the default text if the user's locale is not saved in the browser.

Procedure

1. Click  > **System Configuration > Application Text**.
2. Click  to access the search filter.
3. Click **Labels**.
4. Search for one of the following labels, and then click the link to edit the application text.
 - For the **Privacy Statement** menu item, specify the name of the menu item in **app.header.privacy.label**.
 - For the **Acceptable Use Policy** menu item, specify the name of the menu item in **app.header.acceptable.use.label**
5. Click the name of the locale code you want to modify, for example, en_US.
6. Type the text that you want to display in the menu.
7. Click **Done**.
8. Specify the URL to display when users click the menu items.
 - a) Click  > **System Configuration > Settings**.
 - b) Edit the following settings:
 - For the **Privacy Statement** menu item, specify the URL of the privacy statement in the **Applications > Common > Privacy Link URL** setting.
 - For the **Acceptable Use Policy** menu item, specify the URL of the acceptable use policy in the **Applications > Common > Acceptable Use URL** setting.
9. Log out and log back in to see your changes.

Tip: To remove a menu item, clear the text in its application text label and remove the URL from its registry setting.

The Custom folder

The **Custom** folder is a container for user-defined keys (such as values returned by computed fields, e-mail text for Notification Reports, and values used by Survey reports).

The keys also provide a means for displaying localized text in the IBM OpenPages with Watson user interface for reports (such as reports that are manually published).

Typically, this folder is populated through the ObjectManager tool. You can add new keys to the **Custom** folder from the **Application Text** page.

To modify localized display text for a key in the **Custom** folder, see [“Modifying application text \(Task Focused UI\)” on page 566](#).

Adding new keys

You can add new keys to the Custom folder for localization.

Note: For Cognos report pages (or JSP report instances) that were manually created using the publishing facility on the IBM OpenPages with Watson server, you can use the values in the Report Name Key and Report Description Key fields on the report page to manually create custom application text keys to localize the name and description of a report after it is created.

Procedure

1. Click  > **System Configuration** > **Application Text**.
2. Click  to access the search filter.
3. Click **Custom**.
4. Click **Add New**.
5. On the add detail page:
 - a) In the **Name** box, type the name of the key.
For example, a report called My Loss Events could have `report.name.my.loss.events` for a report name key or `report.description.my.loss.events` for a report description key.
 - b) Optionally, type a description of the key.
 - c) In the **Default Label** box, type the text that will be displayed, by default, if no translated text is provided.
 - d) Type the translated text you want displayed for each locale.
 - e) Click **Done**.

Modifying custom keys

You can modify custom keys.

Procedure

1. Click  > **System Configuration** > **Application Text**.
2. Click  to access the search filter.
3. Click **Custom**.
4. Click the link for the locale code you want to update.
5. Type the translated text you want displayed for that locale.
6. Click **Done**.

Chapter 18. Reporting periods, object resets, and rulesets

A reporting period is a "snapshot" of the current state of the repository, usually created when the documentation phase of a quarter or year is complete and ready for attestation. Object resets are a way to automatically modify objects that exist in the IBM OpenPages with Watson repository. Object resets are rule-based operations that are contained in a ruleset.

Reporting periods

Past reporting periods can be viewed and reported on from any time in the future without rolling back the changes made to the repository after the reporting period was created. After a reporting period is created, the existing report is carried forward to the current reporting period and can be modified without altering the state of the earlier reporting period's data. Only one reporting period at a time can be "Active".

How reporting periods are handled in the Task Focused UI and the Standard UI

Administrators can create, finalize, and delete reporting periods in either the Task Focused UI or the Standard UI. Changes made in one interface are immediately reflected in the other.

Functionality between the two interfaces is the same with the exception of differences around active reporting periods:

- Administrators can create and finalize active reporting periods in either user interface.
- User can view data, for example, in dashboards and for objects, for the current reporting period and past reporting periods in the Task Focused UI. However, users cannot select nor view data for the active reporting period in the Task Focused UI.
- User can view data for the active reporting period, the current reporting period, and past reporting periods in the Standard UI.
- Users can reapply and finalize active reporting periods per business entity only in the Standard UI.

Object resets

The most common use of the object reset functionality is to "reset" all of your objects at the beginning of a new reporting period. For example, each quarter you have controls and tests that need to be reviewed and performed. The results of those tasks are recorded by updating the properties and attachments of the appropriate objects. After all quarterly tasks are completed, and the quarter is finished, you archive all of the results into a reporting period and prepare for the new quarter. However, the existing objects still display the test results and changed properties of the previous quarter. If you are planning to reset your data as part of the beginning of a new reporting period, you will have to archive the existing data to a reporting period.

Rather than modify the objects by hand, you can use the object reset capability to take your existing objects and modify their properties based on the rules in your ruleset.

While object resets work well with the reporting period capability of the OpenPages with Watson application, object resets do not require the existence of a reporting period to be used.

Resets can be started in either the Task Focused UI or the Standard UI. For information, see [“Performing the object reset” on page 592](#).

Active reporting periods and operational limitations

Active reporting periods are essentially in the process of being closed (or "finalized").

An active reporting period affects behavior in the Standard UI as follows.

- An active reporting period can be reapplied at any business entity level to synchronize the business entity and its children with the current reporting period.
- Filtering behavior:
 - Only filters that use system fields (such as, Name or Description) will work.
 - All objects on Filtered List View, Activity View, and Home pages are generally displayed, unless a system-field filter is applied to a particular view.
 - When you use the Grid View, only the top level objects are displayed.
- Reporting behavior: Reports cannot run against an active reporting period. You can only run reports against the current reporting period and any finalized past reporting periods.
- The following operations cannot be performed during an active reporting period on object types that have their own folders (such as Business Entities, object types that are part of the security model, and self-contained object types):
 - Move operations
 - Rename operations
- The Delete operation cannot be performed during an active reporting period on any object types.

Finalized reporting periods

After an active reporting is finalized, the contents of that reporting period cannot be altered. Any changes to the objects or files will only be reflected in the current reporting period.

This allows administrators to create the next reporting period ahead of time and then apply it incrementally to different areas of their documentation project when each area is ready to be finalized.

Reporting period interactions

You can interact with the reporting schema, the ACL, and the change history for a reporting period.

Reporting schema interactions

By default, the reporting schema is only populated with the data from the current reporting period.

To populate the reporting schema with data from previous reporting periods you must enable the **Populate Past Periods** setting and recreate the reporting schema (see, [“Populating past reporting periods”](#) on page 160).

ACL interactions

When viewing objects, your existing ACLs control which objects you can view in the current reporting period and in past reporting periods. If your access permissions change in the current reporting period, you will be able to view the newly accessible items in past reporting periods, and you will not be able to view items to which you have lost permissions, even if in past reporting periods you had access to them.

Regardless of your access permissions, you are never allowed to add, edit or remove objects and/or files from past reporting periods.

Change history interactions

When viewing a change history for an object, only the changes made during the currently selected reporting period are shown. You can view the change history for past reporting periods, but only the change activities for that reporting period will be shown.

You cannot view change histories for multiple reporting periods on the same page.

Using System Admin Mode with reporting periods

When you create, finalize, or delete reporting periods, you need to be in System Admin Mode (SAM).

For more information, see [“Enabling and disabling System Admin Mode” on page 71.](#)

Reporting period permissions and settings

To manage reporting periods, the user performing the reporting period operation must belong to a group with the specific application permissions. The amount of time after a reporting period is created in which the reporting period can be deleted is set in the *Delete Interval* setting

Reporting period permissions

Administrators with the Reporting Periods application permission can create, modify, and delete reporting periods in both the Task Focused UI and the Standard UI.

For the Standard UI, there are two sub-permissions for reporting periods:

- **Finalize** - allows members of the group to finalize reporting periods on Business Entities. Users will only be able to finalize reporting periods on Business Entities to which they have viewing permissions.
- **Reapply** - allows members of the group to update the active reporting period to represent the current state of a Business Entity.

Deletion period setting

It is possible to configure the amount of time after a reporting period is created in which the reporting period can be deleted. This property is set in the *Delete Interval* setting and defaults to 7 days after the reporting period is created.

For details see, [“Modify the deletion interval for a reporting period” on page 602.](#)

Creating and finalizing a reporting period (Task Focused UI)

You can create active and finalized reporting reports.

Before you begin

To create a new reporting period, you must have the reporting periods application permission.

Enable System Admin Mode. Click  > **Enable System Admin Mode**.

About this task

You can create two kinds of reporting periods:

- Active reporting periods

Create an active period if further data changes are expected.

If an active reporting period already exists, you cannot create a new reporting period.

- Finalized reporting periods

Create a finalized reporting period if no further data changes are expected and there is not need to reapply portions of the object hierarchy before finalization.

Procedure

1. Click  > **System Configuration** > **Reporting Periods**.

Or, in 8.2.0.3 and earlier, click  > **Reporting Periods** > **Reporting Periods**.

2. To create an active reporting period:

- a) Click **Add Active**.
- b) Enter the information and click **Create**.

The new reporting period displays with a status of "Active".

Note: If you have any standalone objects in your system (objects that were not created in the context of a business entity hierarchy) they will be immediately finalized when the reporting period is created.

- c) Use tasks in the Standard UI to view and change data in the active reporting period. For more information, see [“Working with the active reporting period \(Standard UI\)” on page 581](#).
- d) After all the changes are made and you are ready to finalize an active reporting period, return to this task. Select the reporting period and click **Finalize**.

3. To create a finalized reporting period.

- a) Click **Add Finalized**.
- b) Enter the information and click **Create**.

The new reporting period displays with a status of "Finalized". You are not able to modify it without deleting the entire reporting period.

- c) Use tasks in either user interface to view data in finalized reporting periods.

Deleting a reporting period (Task Focused UI)

After you create a reporting period, occasionally you may have to delete it to reflect last-minute changes to your financial close, or due to a mistake in the name (for example, wrong quarter, wrong year, and so forth).

The current reporting period can never be deleted.

An active reporting period can be deleted at any time.

A finalized reporting period can be deleted for a configurable amount of time after the reporting period is created. For details on this setting, see [“Modify the deletion interval for a reporting period” on page 602](#).

- If the deletion period has **expired**, then the finalized reporting period cannot be deleted.
- If the deletion period has **not expired**, then the finalized reporting period can be deleted.

Note: The default period for deletion of a finalized reporting period is seven days after finalization.

Before you begin

Enable System Admin Mode. Click  > **Enable System Admin Mode**.

Procedure

1. Click  > **System Configuration** > **Reporting Periods**.

Or, in 8.2.0.3 and earlier, click  > **Reporting Periods** > **Reporting Periods**.

2. Select the reporting periods you want to delete.

3. Click .

If  is not displayed, the deletion period for that reporting period has expired. However, you can retroactively change the deletion period setting.

Creating a reporting period (Standard UI)

You can create active reporting reports.

Before you begin

To create a new reporting period, you must have the reporting periods application permission.

Enable system admin mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71.](#)

About this task

If an active reporting period already exists, you cannot create a new reporting period.

Procedure

1. From the menu bar, select **Administration** and click **Reporting Periods**.
2. Click the **Add Active** icon.
3. Enter the necessary information and click **Create**. You are returned to the Reporting Periods page and the new reporting period is listed in the table with a status of "Active".
4. Click **Refresh** to update the current value of the Status field.

Results

After adding a new reporting period, the reporting period will be added to the Reporting Period selection list on each overview and object page.

Note: If you have any standalone objects in your system (objects that were not created in the context of a business entity hierarchy) they will be immediately finalized when the reporting period is created.

For information about deleting reporting periods, see [“Deleting a reporting period \(Task Focused UI\)” on page 580.](#) Deletion follows the same rules in both user interfaces. In the Standard UI, select a reporting period and click **Delete**.

Creating a finalized reporting period (Standard UI)

You can create finalized reporting periods.

Before you begin

Enable system admin mode. For more information, see [“Enabling and disabling System Admin Mode” on page 71.](#)

About this task

You may know that you will not need to edit a reporting period further, and do not need to reapply portions of the object hierarchy before finalization. In this case, you can use the **Add Finalized** icon to create a new reporting period and immediately finalize it. After the reporting period is created you will not be able to modify it without deleting the entire reporting period.

Procedure

1. From the menu bar, select **Administration** and click **Reporting Periods**.
2. Click the **Add Finalized** icon.
3. Enter the label and description for the new reporting period and click **Create**.

Working with the active reporting period (Standard UI)

When an active reporting period is created, it is applied to all of the objects (resources) in the IBM OpenPages with Watson repository.

While a reporting period is active, there are three actions you can take:

- Reapply the reporting period.

For more information, see [“Reapplying the active reporting period to a business entity \(Standard UI\)” on page 582.](#)

- Finalize the reporting period on a business entity-by-business entity case.

For more information, see [“Finalizing a reporting period for a specific business entity \(Standard UI\)” on page 583.](#)

- Finalize the entire reporting period.

For more information, see [“Finalizing a reporting period \(Standard UI\)” on page 583.](#)

When you reapply a reporting period, it updates the "checkpoint" created by the reporting period to include the current state of the business entity (and its children).

When you finalize a reporting period, it freezes the reporting period and prevents any more updates through reapplying the reporting period.

Before you begin

To view active reporting periods, the end user must be a member of the `ActiveReportingPeriodAdministrators` group.

After you associate an end user with this group, the **Reporting Period** option becomes available after the user logs off and log on again.

About this task

You can create, finalize, and delete active reporting periods in both the Task Focused UI and the Standard UI. However, you can only view and change data in an active reporting period in the Standard UI.

Reapplying the active reporting period to a business entity (Standard UI)

Reapplying a reporting period updates the reporting period version of the entity (and its associated hierarchy of objects) to match the current "live" version. Reapplication of the reporting period can be done at any level of the business entity hierarchy, and will only affect the children of the currently viewed business entity.

Procedure

1. Navigate to the business entity you want to be the root of the reapplied reporting period.
2. Select the active reporting period from the list.
3. Click the **Re-Apply** icon to update the business entity and all of its children to their current "live" version.
4. On the locks page, if you want to remove all locks on the selected business entity after the reapply operation, select the Remove all Locks option.

Results

For example, if you have a business entity with the field "Entity in Scope?" set to "Yes" and you create an active reporting period, when you view that business entity in that reporting period you will see "Yes" as the value.

If you then change the value of Entity In Scope to "No" in the Current Reporting Period (the live data), and you want to update the entity in the active reporting period, you can reapply the active reporting period and the value of Entity In Scope will be updated to "No".

Note: There is no way to reverse a reapplication of a reporting period or to only pick up some of the modifications made to the children of the business entity, so be careful when reapplying a reporting period.

Finalizing a reporting period for a specific business entity (Standard UI)

After you are certain that no more changes need to be made to a business entity and its descendants, you can finalize the reporting period for that business entity.

If even one business entity is not finalized, the reporting period remains active.

Procedure

1. Navigate to the business entity you want to be the root of the finalized reporting period.
2. At the beginning of the page, select the active reporting period from the list and click the >> icon.
3. Click the **Finalize** icon to prevent any further changes to the business entity and all of its child objects.

Finalizing a reporting period (Standard UI)

After you are certain that no more changes need to be made, you can finalize the active reporting period.

After you finalize an entire reporting period, it ceases to be active. Only then can you create a new active reporting period.

Before you begin

Enable system admin mode. For more information, see [“Enabling and disabling System Admin Mode”](#) on page 71.

Procedure

1. From the menu bar, select **Administration** and click **Reporting Periods**.
2. Click the name of the active reporting period.
3. Click the **Finalize** icon to finalize the entire reporting period. The status of the reporting period changes to Finalizing.
4. Click **Refresh** to update the current value of the Status field.

Note: You cannot undo a finalize operation without removing the entire reporting period. Depending on the size of your repository, it may take a significant amount of time to finish the finalizing operation.

Object resets

Object resets are a way to automatically modify objects that exist in the IBM OpenPages with Watson repository.

The most common use of the object reset functionality is to "reset" all of your objects at the beginning of a new reporting period. For example, each quarter you have controls and tests that need to be reviewed and performed. The results of those tasks are recorded by updating the properties and attachments of the appropriate objects. After all of these quarterly tasks have been completed, and the quarter is finished, you archive all of the results into a Reporting Period and prepare for the new quarter. However, the existing objects still display the test results and changed properties of the previous quarter.

Rather than go in and modify the objects by hand, you can use the object reset functionality to take your existing objects and modify their properties based on the rules in your ruleset.

While object resets work well with the reporting period capability of the OpenPages with Watson application, object resets do not require the existence of a reporting period to be used.

Object resets on file attachments

You can only use object resets to delete objects that are JSP-based, not attachments available when using the **Browse Files** option. For example, if you use an object reset on SOXDocument, you see the following error:

```
VALIDATION ERROR (Line: 8 Column: 55): Content Type (SOXDocument)
must be JSP-based to be referenced in an Object Delete rule.
```

Suppose that you have files that are attached to test results. You can configure the settings to delete attachments when test results are deleted. To delete the SOXDocument objects, you can add SOXDocument to the **Cascade Delete** setting to delete the files that are associated with the test results during the object reset rule to delete test results.

Object resets on system fields

When modifying fields or using fields within <criteria> tags, you may not use "system" fields. System fields are the fields common to all object types, such as name, description, or creator. Field modifications and ruleset criteria must use custom fields (non-system fields). If the field you want does not appear in a field group for the appropriate object type, you cannot use it in your ruleset.

Object resets on currency fields

If you use an object reset rule to update the value of the Local Currency Code of a currency field, the Exchange Rate and Base Amount are not updated to match the new Local Currency Code value.

While the Base Amount is calculated using the Local Currency Code and the Exchange Rate, it will not change because the Exchange Rate has not been modified and the number of displayed fraction digits for the currency has not been changed. In order to see a change in the Base Amount, you must include a rule to update the Exchange Rate or modify the number of displayed fraction digits.

Preparing your data

Before an object reset is performed, you will need to perform a few tasks to help ensure that the reset procedure goes smoothly.

- Back up your OpenPages with Watson data before running an object reset.
- If you plan on archiving your changes to a reporting period, you will need to set up the reporting period before running the object reset.

Creating a ruleset

Object resets are rule-based operations on the objects in your IBM OpenPages with Watson repository. The rules that govern how an object reset will affect your data are contained in a ruleset file.

A ruleset is a set of rules contained in an XML loader file that is created outside of the OpenPages with Watson application. Multiple rulesets can be included in a single XML file. The ruleset loader file is loaded into the system through the ObjectManager loader tool. After the ruleset is imported, it can be selected during the Specify Options step of the Object Reset guided action.

When you use ObjectManager loader tool to import security rules, the entire ruleset is loaded and replace existing security rules that have the same name as a imported rule. Before importing security rules, export your existing rules first.

Object Resets can modify objects in three ways: modifying the value of a property, deleting an object, and disassociating two objects.

When creating a ruleset, you must know the bundles, properties, and property values you are modifying and match them exactly. If you do not specify a valid property or property value, the property will not be modified.

Note: Before creating a final ruleset to use for your reset session, it can be extremely helpful to create simple rulesets that contain a single rule from your final ruleset. Running these single rulesets against a known data set can verify the accuracy of each rule before attempting a massive modification of your data.

To create the ruleset file, create a new XML file. Save the file with the following naming convention:

```
<file-identifier>-op-config.xml
```

Sample ruleset

The following XML is a sample ruleset.

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.20">
  <ruleSets>
    <ruleSet name="Quarterly Reset"
      description="Rule set to be executed at the beginning of each
and every quarter"
      type="Object Reset">
      <rule name="Rule 1"
        description="Property Update rule setting a property"
        type="Property Update">
        <propertyUpdateRule contentType="SOXControl">
          <bundle name="SOXControl">
            <property name="Design Effectiveness"
              useDefaultValue="false">
              <propertyValue name="Not Rated"/>
            </property>
          </bundle>
        </propertyUpdateRule>
      </rule>

      <rule name="Rule 2"
        description="Property Update rule setting a collection of
properties (including a multi-valued one)."
        type="Property Update">
        <propertyUpdateRule contentType="SOXRisk">
          <bundle name="SOXRisk">
            <property name="Assertions"
              useDefaultValue="false">
              <propertyValue name="Existence"/>
              <propertyValue name="Rights and Obligations"/>
            </property>
            <property name="Impact"
              useDefaultValue="false">
              <propertyValue name="Unknown"/>
            </property>
          </bundle>
        </propertyUpdateRule>
      </rule>

      <rule name="Rule 3"
        description="Object Delete rule"
        type="Object Delete">
        <objectDeleteRule contentType="SOXTestResult"/>
      </rule>

      <rule name="Rule 4"
        description="Object Delete rule with criteria"
        type="Object Delete">
        <objectDeleteRule contentType="SOXIssue"/>
        <criteria logicalOperator="or">
          <criterion bundle="SOXIssue"
            property="Status"
            operator="=">
            <propertyValue name="Closed"/>
          </criterion>
        </criteria>
      </rule>
```

```

        <rule name="Rule 5"
              description="Object Disassociate rule"
              type="Object Disassociate">
          <objectDisassociateRule parentContentType="SOXRisk"
                                childContentType="SOXDocument"/>
        </rule>
      </ruleSet>
<!--sample Reset Ruleset for a currency property-->
<ruleSet name="Your_Ruleset_Name"
          description="Reset a currency property"
          type="Object Reset">
  <rule name="Reset a currency property"
        description=""
        type="Property Update">
    <propertyUpdateRule contentType="SOXAccount">
      <bundle name="OPSS-Account_Annualized Value">
        <property name="Annualized Value_LA"
                  useDefaultValue="false">
          <propertyValue name="1.0"/>
        </property>
      </bundle>
      <bundle name="OPSS-Account_Annualized Value">
        <property name="Annualized Value_LC"
                  useDefaultValue="false">
          <propertyValue name="AED"/>
        </property>
      </bundle>
      <bundle name="OPSS-Account_Annualized Value">
        <property name="Annualized Value_ER"
                  useDefaultValue="false">
          <propertyValue name="1.0"/>
        </property>
      </bundle>
    </propertyUpdateRule>
  </rule>
</ruleSet>
</ruleSets>
</openpagesConfiguration>

```

Ruleset tag library

Use the following XML tags to build a ruleset.

[openpagesConfiguration](#)

[ruleSets](#)

[ruleSet](#)

[rule](#)

[propertyUpdateRule](#)

[bundle](#)

[property](#)

[objectDeleteRule](#)

[objectDisassociateRule](#)

[criteria](#)

[criterion](#)

[propertyValue](#)

<openpagesConfiguration>

Description: Progenitor tag for the loader file contents. All other tags are contained within the <openpagesConfiguration> tag.

Parent Tags: None.

Child Tags: <ruleSets>

Syntax:

```
<openpagesConfiguration xmlFormatVersion="1.15">
</openpagesConfiguration>
```

Attributes:

- xmlFormatVersion

Version of the IBM OpenPages with Watson XML DTD.

<ruleSets>

Description: Container tag for one or more ruleSet tags.

Parent Tags: <openpagesConfiguration>

Child Tags: <ruleSet>.

Syntax:

```
<ruleSets>
</ruleSets>
```

Attributes: None.

<ruleSet>

Description: A ruleset is a collection of rules that will be executed when the ruleset is selected during a Reset session. Each ruleset is displayed in the IBM OpenPages with Watson user interface as a separate entry in the list of Rulesets.

Parent Tags: <ruleSets>

Child Tags: <rule>

Syntax:

```
<ruleSet name="Name"
         description="Description"
         type="Object Reset">
</ruleSet>
```

Attributes:

- name

An identifying name for the ruleset. Will be displayed in the OpenPages with Watson user interface. The maximum length for the ruleset name attribute is 255 bytes (not characters).

- description

A description of the function of the ruleset. The maximum length for the ruleset name attribute is 2000 bytes (not characters).

- type

The type of ruleset. Currently, there is only one type - "Object Reset".

<rule>

Description: Each <rule> tag contains a single rule that will be applied to the IBM OpenPages with Watson data when the ruleset is selected and a Reset session is initiated.

Parent Tags: <ruleSet>

Child Tags: <propertyUpdateRule>, <objectDeleteRule>, <objectDisassociateRule>, <criteria>

Syntax:

```
<rule name="Name"
      description="Description"
      type="[Property Update|Object Delete|Object Disassociate]"
/>
```

Attributes:

- name
The name of the rule. The maximum length for the rule name attribute is 255 bytes (not characters).
- description
A description of the function of the rule. The maximum length for the rule name attribute is 2000 bytes (not characters).
- type
The type of rule. There are three types of rules: Property Update, Object Delete, and Object Disassociate.

<propertyUpdateRule>

Description: The <propertyUpdateRule> tag defines a rule that modifies the value of an existing property on a certain object type. Unless modified by the use of the <criteria> tag within the same <rule> tag, all objects of the specified object type within the scope of the Reset will be updated.

Parent Tags: <rule>

Child Tags: <bundle>

Syntax:

```
<propertyUpdateRule contentType="">
</propertyUpdateRule>
```

Attributes:

- contentType
Specifies the object type that the rule will be applied to. Must match a valid IBM OpenPages with Watson object type.

<bundle>

Description: The <bundle> tag specifies which bundle contains the property to be modified.

Parent Tags: <propertyUpdateRule>

Child Tags: <property>

Syntax:

```
<bundle name=""
/>
```

Attributes:

- name
The name of the bundle whose property will be modified.

<property>

Description: The <property> tag is used inside a <bundle> tag to specify the property that will be updated.

Parent Tags: <bundle>

Child Tags: <propertyValue>

Syntax:

```
<property name="">
  useDefaultValue="[true|false]"
  [<propertyValue>
    <propertyValue>]
</property>
```

Attributes:

- name

The name of the property to be updated.

- useDefaultValue

Specifies whether the property should be updated to reflect the default value of the property (if one exists). If no default value exists, the property is not updated.

<objectDeleteRule>

Description: The <objectDeleteRule> tag is used to specify an object type for deletion. Unless modified by the use of the <criteria> tag within the same <rule> tag, all objects of the specified object type within the scope of the Reset will be deleted.

Parent Tags: <rule>

Child Tags: None.

Syntax:

```
<objectDeleteRule contentType="" />
```

Attributes:

- contentType

Specifies the object type to be deleted. All objects of this type within the scope of the Reset are deleted.

<objectDisassociateRule>

Description: The <objectDisassociateRule> tag is used to disassociate an object type from another object type. If you use the <criteria> tag with this rule type, the criteria must be based on the child's property values. You cannot base a rule on properties or property values belonging to the parent object type.

Parent Tags: <rule>

Child Tags: None.

Syntax:

```
<objectDisassociateRule parentContentType=""
  childContentType="" />
```

Attributes:

- parentContentType

Identifies the parent object type that the child object type is associated with.

- childContentType

Identifies the child object type to be disassociated. Any objects of the child object type associated with objects of the parent object type within the scope of the Reset will be disassociated from the parent object.

<criteria>

Description: The <criteria> tag is used to refine the behavior of a rule by specifying the standards that need to be met in order to invoke the rule. The criteria tag can contain one or more <criterion> tags that will be judged when deciding whether to apply the rule to a specific object.

It should be noted that criteria can only be applied in a "positive" manner - that is, if the criteria are met, the rule will be used. You cannot specify a rule where if the criteria are met, the rule is NOT applied.

Parent Tags: <rule>

Child Tags: <criterion>

Syntax:

```
<criteria logicalOperator="[and|or]">
```

Attributes:

- logicalOperator

Specifies whether all of the criterion ("and") will be used to determine whether the rule will be applied to the object, or if only one of the criterion ("or") needs to be satisfied.

<criterion>

Description: The <criterion> tag allows the user to specify a property and value(s) that must match the evaluation specifications set in the <criterion> tag.

Use a maximum of three criterion within a single <criteria> tag. Adding additional criterion will increase the processing time required to complete the Reset.

Parent Tags: <criteria>

Child Tags: <propertyValue>

Syntax:

```
<criterion bundle=""
           property=""
           operator="[=|<>|<|>|<=|>=|like]"
  <propertyValue="" />
  [<propertyValue="" />]
</criterion>
```

Attributes:

- bundle

The property bundle containing the property to be evaluated.

- property

The property name of the property to be evaluated.

- operator

Specifies the manner in which the value of the property will be evaluated. Valid operators are equal (=), not equal (< >), greater than (>), less than (<), greater or equal to (>=), less than or equal to (<=), and "like".

Only the equal, not equal, and "like" operators can be used with string variables.

Note: The "like" parameter allows the use of wild cards in the <propertyValue> tag. These wild cards consist of the "%" and "_" symbols, which are passed to a SQL database query against the database. The percent mark (%) symbol is used to represent any number of characters in a location, while the underscore (_) character is used to represent any single character in a location.

For SQL tool information, see [“Database tool information” on page xxxi](#).

Note: The <propertyValue> referenced in a <criteria> tag cannot be null (or empty).

<propertyValue>

Description: The <propertyValue> tag performs two functions, depending on its location. The Boolean property value must be all lowercase. For example, "true" is correct, "True" is incorrect.

If the <propertyValue> tag is contained inside a:

- <property> tag, it specifies the new value (or values) for the updated property.
- <criteria> tag, it specifies the relevant property to be considered when applying the criteria.

Note: The <propertyValue> referenced in a <criteria> tag cannot be null (or empty).

If you are modifying an enumerated string (drop-down list) property that is multi-selectable, you can place multiple <propertyValue> tags inside the <property> tag. When the rule is processed, all of the <propertyValue> tags will be evaluated, and the property will be modified to select all of them.

Parent Tags: <property>, <criteria>

Child Tags: None.

Syntax:

```
<propertyValue name="" />
```

Attributes:

- name

Specifies the value of the property. The maximum length for the property value's name attribute is 2000 bytes (not characters).

Loading the ruleset

After you have finished creating the ruleset loader file, you will need to use the ObjectManager tool to load the ruleset into the IBM OpenPages with Watson system.

If you load a ruleset with the same name as an already-loaded ruleset, the ruleset will be overwritten with the new rules. To return to an earlier version of the ruleset, you would have to re-load the original ruleset loader file. Rulesets are not "version-controlled".

Procedure

1. Open a command or shell window on the OpenPages with Watson server.
2. Navigate to the <OP_Home> directory.

Where: <OP_Home> represents the installation location of the OpenPages with Watson application. By default, <OP_HOME> is c:\IBM\OpenPages on Windows or /opt/IBM/OpenPages on Linux.

3. Run the following command on a single line:

```
ObjectManager load config OpenPagesAdministrator <password> <path-to-ruleset-XML-file>  
<file-identifier>
```

where

<password> is the password to the OPAdministrator user account.

<path-to-ruleset-XML-file> is the full path to the ruleset file you created.

<file-identifier> is the portion of the ruleset file name preceding "-op-config.xml". For example, if you created a ruleset file called "ruleset-op-config.xml", the <file-identifier> in the ObjectManager command is "ruleset".

4. The ruleset is now loaded. If you created multiple ruleset files, repeat this procedure for each of them.
5. If you encounter errors, read the log file to determine the cause of the error and fix it, then re-run the command in Step 2.

Performing the object reset

After you load the ruleset that you are using for the Object Reset, you must log in to the system and begin the Reset.

Start resets from either user interface

Resets can be started in either the Task Focused UI or the Standard UI. Changes that made in one interface are immediately reflected in the other.

Access permissions and access

The user who runs the Reset must have the Object Reset application permission and the proper access to modify the data. The same permissions are applied in both the Task Focused UI and the Standard UI.

If the user does not have the Object Reset permission, they are not able to see Object Resets on the menu.

Configuring the ruleset parameters

Before running the Reset, there are some configuration parameters that should be set. In general, these settings need to be set only one time before your first time initiating a Reset, but you may want to change them for different entity trees or ruleset behavior.

Access the following Object Reset settings in the **Applications > Common > Object Reset** folder:

- **Logging Level** - this setting controls how much information is displayed. For configuration details, see [“Changing the logging level” on page 624](#).
- **Check ACL** - this setting controls whether the Reset occurs against all or only some of the objects contained within the scope of the Reset session. For configuration details, see [“Obeying ACL restrictions” on page 624](#).
- **Ignore Locks** - this setting controls whether existing locks on objects are honored when running the Reset. For configuration details, see [“Obeying locking restrictions” on page 625](#).
- **Continue on Error** - this setting controls whether the Reset session will log errors and continue to run or halt processing. For configuration details, see [“Continuing on error” on page 624](#).

Starting the object reset (Task Focused UI)

When you reset objects, watch the status of the job and review the results for errors and warnings.

About this task

When you reset objects, watch the status of the session and review the results for errors and warnings.

The possible values for the **Status** field are Initiated, In Progress, Completed, or Failed.

The "Failed" status is shown only if the system is set to stop the reset if errors are encountered. If the system is set to continue on errors, then when the reset is completed, the "Completed" status is shown. Any errors that occurred during the reset are captured in the Reset Session Log.

Note: If you have chosen to obey ACL restrictions, the user must have the permissions to modify the objects within the scope of the Reset. If the user does not have sufficient permissions, warning messages will be generated in the log, and the objects will not be modified.

Procedure

1. Click  > **System Configuration** > **Object Resets**.
Or, in 8.2.0.3 and earlier, click  > **Reporting Periods** > **Object Resets**.
2. Click **New Reset**.
3. Enter a name and description for the new reset.
4. Select a ruleset from the list of available rulesets.
5. Click Choose next to **Reset Scope**.
6. Choose the Business Entities to which the Reset will be applied by selecting the check boxes next to the entity names. Click **Done**.
7. Click **Start Reset**.
The reset starts.
8. Track the progress of the reset session by monitoring the **Status** column of the table.

Results

When the reset session is finished, a new reset session is added to the list.

What to do next

Click the reset session and review the results:

- Click the **Information** tab to view object reset details. For information, see [“Viewing reset session detail information”](#) on page 593.
- Click the **Log** tab to view errors and warnings. For information, see [“Viewing reset session log information”](#) on page 594.

Refresh the reporting database. For information, see [“Refreshing the reporting database after the reset”](#) on page 595.

Viewing reset session detail information

You can view details about a reset session that is finished.

Click the name of an object reset session. The following information is displayed:

Name - The name of the Reset Session.

Description - The description of the Reset Session (set during the creation procedure)

Ruleset Name - The name of the Ruleset that was applied during this session.

Created - The time and date the Reset Session was created.

Start Date - The time and date the Reset began.

End Date - The time and date the Reset finished.

Status - The current status of the Reset. The Status can be one of the following values:

- **Initiated** - The Reset has been initialized, and is preparing to modify your data.
- **In Progress** - The Reset is currently modifying the selected data.
- **Completed** - The Reset finished successfully. Depending on whether the Reset was set to continue on errors, some errors may be reported in the Session Log.

- **Failed** - The Reset did not finish, because errors were encountered. Check the Session Log for details on what errors occurred.

Created By - The user that initiated the Reset Session.

Scope - The Business Entities that were modified by the Reset.

Logging Level - The level of detail that will be displayed in the Session Log. Can be one of the following values:

- **Low** - display error messages only
- **Medium** - display any error messages and any warning messages.
- **High** - display any errors, warnings, and any informational or diagnostic messages.

Continue on Error - Whether the Reset Session will log errors and continue to run, or whether the error will be logged and the session will halt. Value will either be "true" or "false".

Check ACLs - Whether the Reset occurs against all objects contained within the scope of the Reset session, or whether the Reset occurs against only those objects that the user who initiated the Reset has access to. It can have a value of "true" or "false".

Ignore Locks - Whether existing locks on objects are honored when running the Reset. A value of "true" means that locks were ignored when running the Reset, and a value of "false" means that locked objects were not modified by the Reset.

Viewing reset session log information

You can view log information about a reset session that is finished.

The level of detail depends on the configuration setting. For details on setting the logging level, see the topic [“Performing the object reset” on page 592](#).

Procedure

Click **Log** on the reset session detail page. This is titled **View Log** in the Standard UI.

The reset session log contains three sections - the error messages section, the warning messages section, and the informational messages section.

Starting the object reset (Standard UI)

When you reset objects, watch the status of the job and review the results for errors and warnings.

About this task

The possible values for the **Status** field are Initiated, In Progress, Completed, or Failed.

The "Failed" status is shown only if the system is set to stop the reset if errors are encountered. If the system is set to continue on errors, then when the reset is completed, the "Completed" status is shown. Any errors that occurred during the reset are captured in the Reset Session Log.

Procedure

1. Log on to the IBM OpenPages with Watson Standard UI as a user with the Object Reset application permission.

Note: If you have chosen to obey ACL restrictions, the user must have the permissions to modify the objects within the scope of the Reset. If the user does not have sufficient permissions, warning messages will be generated in the log, and the objects will not be modified.

2. Click **Administration > Object Resets**.
3. Click **Start New Reset** at the beginning of the table to create a new reset.

4. Enter a name and description for the new reset.
5. Select a ruleset from the list of available rulesets.
6. Click **Next** to display the Reset Scope page.
7. Choose the Business Entities to which the Reset will be applied by selecting the check boxes next to the entity names. After you select the Business Entities, click **Start Reset**.
The reset starts.
8. Track the progress of the reset session by monitoring the **Status** column of the table.

Results

When the reset session is finished, a new reset session is added to the list.

What to do next

Click the reset session and review the results:

- The **Object Reset Detail** page shows information about the session. For information, see [“Viewing reset session detail information ” on page 593](#).
- Click **View Log** to view errors and warnings. For information, see [“Viewing reset session log information” on page 594](#).

Refresh the reporting database. For information, see [“Refreshing the reporting database after the reset” on page 595](#).

Refreshing the reporting database after the reset

After you perform an object reset, refresh the reporting database so that users who run third-party reports will immediately see the changes.

If your users are using the reporting schema, you do not need to perform a reporting schema refresh. The IBM OpenPages with Watson reports will automatically see the changes.

For detailed information on performing a reporting database refresh, see [Chapter 6, “Managing the reporting schema ,” on page 159](#).

Exporting rulesets to an XML file

You can export all of the object reset rulesets to an XML file using ObjectManager. In order to do this, you must have file access to the IBM OpenPages with Watson server.

This procedure will export ALL defined rulesets. Exporting rulesets does not remove them from the OpenPages with Watson application; they will still be available for use after they are exported.

Procedure

1. Back up the `ObjectManager.properties` file.

Note: The `ObjectManager.properties` file is located in the root installation folder of your OpenPages with Watson installation. By default, this is `c:\OpenPages`.

2. Open the `ObjectManager.properties` file in a text editor.
3. Locate the following block of settings in the file:

```
configuration.manager.dump.modules=true
configuration.manager.dump.file.types=true
configuration.manager.dump.bundle.types=true
configuration.manager.dump.file.upload.content.types=true
configuration.manager.dump.jsp.based.content.types=true
configuration.manager.dump.content.type.relationship.sets=true
```

```
configuration.manager.dump.app.permissions=true
configuration.manager.dump.actors=true
configuration.manager.dump.actor.group.memberships=true
configuration.manager.dump.actor.object.profile.associations=true
configuration.manager.dump.non.form.based.resources=true
configuration.manager.dump.form.based.content.types=true
configuration.manager.dump.form.based.resources=true
configuration.manager.dump.channels=true
configuration.manager.dump.resource.sets=true
configuration.manager.dump.associated.resources=false
configuration.manager.dump.rule.sets=true
configuration.manager.dump.rule.set.execute.sessions=true
configuration.manager.dump.registry=true
configuration.manager.dump.object.profiles=true
configuration.manager.dump.locales=true
configuration.manager.dump.application.string.key.categories=true
configuration.manager.dump.application.string.keys=true
configuration.manager.dump.application.strings=true
configuration.manager.dump.error.strings=true
configuration.manager.dump.object.strings=true
configuration.manager.dump.job.types=true
configuration.manager.dump.currency.exchange.rates=true
configuration.manager.dump.currencies=true
configuration.manager.dump.query.definitions=true
```

4. Modify each line to have a false value, except the line that reads:

```
configuration.manager.dump.rule.sets=true
```

5. Make sure that the following setting has a value of false:

```
configuration.manager.migrate.configuration.objects
```

6. Save the file and exit the editor.
7. Open a Command Prompt window.
8. Navigate to the <OP_Home> directory.

Where:

<OP_Home> is the installation location of the OpenPages with Watson application. By default, this is c:\OpenPages.

9. Run the following command on a single line:

```
ObjectManager dump config OpenPagesAdministrator <password>
<path-to-xml-file> <file-identifier>
```

where

<password> is the password to the OPAdministrator user account.

<path-to-XML-file> is the full path to the ruleset file you created.

<file-identifier> is the portion of the ruleset file name preceding "-op-config.xml". When the XML file is created, the file name will append "-op-config.xml" to the end of the filename. For example, if you specified a <file-identifier> called "ruleset", the generated XML file would be named "ruleset-op-config.xml".

10. A new XML file is generated in the specified location that contains only the latest version of the rulesets that exist in the application at the time of the export.

Note: Be sure to "reset" the ObjectManager.properties file to its original contents - otherwise, your scheduled backups using ObjectManager will only export the rulesets.

Chapter 19. Viewing the Configuration and Settings page

Settings control the functionality of numerous aspects and features in IBM OpenPages with Watson.

Settings can be defined in either the Task Focused UI or the Standard UI. Changes made in one interface are immediately reflected in the other. For more information, see:

- [“Managing settings \(Task Focused UI\)” on page 597](#)
- [“Modifying settings \(Standard UI\)” on page 598](#)

For information about working with settings in data loader files, see [“Paths for settings in data loader files” on page 599](#).

Managing settings (Task Focused UI)

Use the Task Focused UI to modify the values for predefined settings and add, copy, and delete custom settings.

Before you begin

To access **Manage Settings** in the Task Focused UI, you must have the Settings application permission set on your account.

About this task

You can use the Task Focused UI to modify all settings, not just those that appear in the Task Focused UI.

You can modify the values for predefined settings. Do not delete any of the predefined settings that are shipped with OpenPages. These settings are required and cause unexpected behavior in the application if they are removed.

You can add your own custom folders and settings. The **Add Setting** and **Delete** icons are hidden by default. Set both Show Hidden Settings and Allow Create and Deleting Settings to true to add and delete settings. You can copy individual settings to another location and copy folders to new folders. When you copy a folder, you can give the new folder a name. The settings and subfolders in the folder are copied to the new folder.

Procedure

1. Click  > **System Configuration** > **Settings**.
2. To find a setting that you want to view or modify, click  to access the search filter.
 - a) Select one or more folders in **Search Scope**.

The folder path displays at the top of the list.
 - b) Optional: Click in the Search box and enter free text. The search returns a results when it finds a match in the name, description, or value of a setting. You can enter single words. For example, enter "hidden" to find all settings with the word "hidden" in the name, description, or value. The Search box text is not case sensitive.
 - c) Locate the setting that you want to modify.

Note: In a folder with many settings, you might want to increase the items per page. You can also go directly to a selected page.
 - d) Click on a setting in the list.

- e) Make your changes in **Value**.
- f) Click **Done**.
The change is saved.
- 3. To add a custom folder, click **Add Folder**.
 - a) Enter a **Name**.
The name should begin with a letter and can contain letters, numbers, space, underbar, and hyphen.
 - b) Click **Choose** and drill down into **Folder Path** to select where to place the new folder.
 - c) Click **Done**.
The folder is added.
- 4. To add a custom setting, click **Add Setting**.
 - a) Enter a **Name**.
 - b) Enter a **Description**.
 - c) Click **Choose** and select a **Folder Path** where the new setting is saved.
 - d) Enter a **Value**.
 - e) Set **Encrypted** to true to make the value of the setting encrypted.
 - f) Click **Add**.
The setting is added.
- 5. To copy a custom setting or folder:
 - a) Select a setting or folder that you want to copy.
 - b) Click **Copy to**.
 - c) Choose a folder where the new setting or folder belongs.
 - d) Click **Done**.
The setting or folder and all of its settings is copied. You can change the description but not the name of the new setting.
- 6. To delete a custom folder or setting:
 - a) Select a custom folder or setting that you want to delete.
 - b) Click **Delete**.
 - c) Click **Done**.
The folder or setting is deleted.

Modifying settings (Standard UI)

You can modify the values for settings in the Standard UI.

Before you begin

To access the **Settings** menu, you must have **Settings** application permission on your account. For more information, see [“Types of application permissions” on page 91](#).

About this task

Tip: You can define settings in the Task Focused UI. For more information, see [“Managing settings \(Task Focused UI\)” on page 597](#).

Procedure

1. Log on to the IBM OpenPages with Watson Standard UI.
2. From the navigation bar, select **Administration > Settings**.

Paths for settings in data loader files

In data loader XML files, the path of a setting begins with `/OpenPages/`. The `OpenPages` folder is hidden in the user interface, but you must include it in the path when you work with settings in a data loader file.

For example, in the user interface, the path to the **Transaction timeout** setting for FastMap is:

Applications > GRCM > FastMap > Transaction timeout.

In a data loader file, the path is `/OpenPages/Applications/GRCM/FastMap/Transaction timeout`. The path is specified in the `name` attribute of the `<registryEntry>` element. The following example shows the syntax:

```
<registryEntry name="/OpenPages/Applications/GRCM/FastMap/Transaction timeout"
  description="The maximum time in seconds that a process can run for."
  hidden="false"
  encrypted="false"
  protected="true"
  value="41600"/>
```

For more information, see [“Creating a data loader file”](#) on page 882.

Applications folder settings

The registry settings in the Application folder represent a select list of individual settings.

All of the following actions are accessed from the Applications folder.

To access the Applications folder, you must have Settings application permission set on your account.

Modify the overview view cache capacity

To enhance performance on an Overview view page, you can change the maximum number of nodes that can be displayed to users in an Overview view by changing the value of the **Overview Cache Capacity** setting.

If the number of nodes that are displayed exceeds the default of 10000, the additional nodes are not displayed. Each cached object requires 1600 bytes of memory.

Applications > GRCM > Caches

Default: 10000

Value: In the **Value** box, type a new numeric value.

The new setting will take effect after you log out and log back in.

Configure the browser cache

Affect the behavior of the browser's back and forward icons by changing the value of the **Disable Browser Cache** setting.

Applications > Common > Configuration > Disable Browser Cache

Default: **false**

Values:

- **true** - the browser's cache is disabled; using the back icon sometimes requires a refresh command for the page to display.
- **false** - the browser's cache is enabled and no refresh action is required; however, the data on the page might be whatever was cached in the browser.

Display the accessibility link

To display a client-specific page with information about accessibility for disabled users, configure the display of the **Accessibility** link in the header pane of the IBM OpenPages with Watson application.

When a user clicks the Accessibility link, the designated page is displayed. By default, the Accessibility link is not displayed in the header pane of the application.

Applications > Common > Accessibility > URL

Default: none

Value: In the **Value** box, type a URL.

For example, you create a page in HTML format that contained information about your company's accessibility policy for disabled users and want this policy to be available to all users through the application. The saved file is named `accessibility.htm` and was copied to the `custom_files` folder, which you created, under the `/sosa` folder location on the server, "machine1".

The URL path that you would enter in the **Value** box might look similar to the following:

```
http://machine1:7009/openpages/custom_files/accessibility.htm
```

Display or hide field guidance

Show or hide field-specific guidance on the Add or Edit page of an object through the **Show Field Guidance** setting.

By default, the **Show Field Guidance** setting is set to display in the application. When a user clicks a question mark icon next to a specific field on an object's Add or Edit page, the field guidance text is displayed.

Applications > Common > Configuration > Show Field Guidance

Default: true

Values:

- **true** - the question mark icon and field guidance text is displayed to users.
- **false** - the question mark icon and field guidance text is hidden from users.

Display or hide system generated field guidance

The **Show System Generated Field Guidance** setting controls whether information about field dependencies and dependent picklists is appended to field guidance.

For this setting to have effect, the **Show Field Guidance** setting must be set to true. If **Show Field Guidance** is false, then no guidance would be shown in any event. For details, see [“Display or hide field guidance” on page 600](#).

Applications > Common > Configuration > Show System Generated Field Guidance

Default: true

Values:

- **true** - shows system-generated dependencies information.
- **false** - suppresses system-generated dependencies information.

Disable the Add New wizard from various launch points

You can disable the **Add New** capability for any or all objects from several launch points within the product. There is a different registry setting for each of the launch points.

These launch points do not prefill parent information. If users find it difficult to select the most appropriate parent information for particular object types, you can disable the **Add New** capability.

Note: The **Object Types Disabled** setting overrides these settings. If an object type is disabled everywhere, there is no need to disable the Add New wizard individually for each launch point. For more information about the **Object Types Disabled** setting, see [“Controlling the availability of object types in the Add New wizard”](#) on page 286.

Table 193. Disabling the Add New wizard	
Setting name	Description
Disable Add New Global Launch Point	Controls whether the Add New button  Add New appears on the menu bar of every page.
Disable Add New Home Page Filtered List Global Launch Points	Controls whether the Add New icon  appears in a pane on the My Work tab on the Home page. When you disable this launch point, users can still use the Add New capability from a row in a pane.
Disable Add New Filtered List View Page Global Launch Points	Controls whether the Add New icon  appears on the Filtered List View/Grid View toolbar. Also controls whether the Add New menu item is displayed in the Grid Actions menu. When you disable this launch point, users can still use the Add New capability from a row in the grid.
Disable Add New Home Page Dashboard Launch Points	Controls whether the Add New capability is enabled from the Home page Dashboard panel launch point.

Applications > GRCM > Add New Wizard > Disable Add New Global Launch Point

Default: none

Values: In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (.). Use the object names and not the object labels. A value of \$ALL\$ disables the launch point for all object types.

Applications > GRCM > Add New Wizard > Disable Add New Home Page Filtered List Global Launch Points

Default: none

Values: In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (.). Use the object names and not the object labels. A value of \$ALL\$ disables the launch point for all object types.

Applications > GRCM > Add New Wizard > Disable Add New Filtered List View Page Global Launch Points

Default: none

Values: In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (.). Use the object names and not the object labels. A value of \$ALL\$ disables the launch point for all object types.

Applications > GRCM > Add New Wizard > Disable Add New Home Page Dashboard Launch Points

Default: none

Values: In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (.). Use the object names and not the object labels. A value of \$ALL\$ disables the launch point for all object types.

Configure file check-out

The file check-out feature locks files to prevent other users from uploading and overwriting changes, or from moving, renaming, or deleting the file while a file is checked out. When the file is checked in, the lock is removed.

You can configure the display of the **Check Out** and **Check In** icons by changing the value of the **Enable File Checkout** setting.

The **Enable File Checkout** setting applies only to the Standard UI. It does not apply to the Task Focused UI.

Applications > GRCM > Enable File Checkout

Default: true

Values:

- **true** - the file check-out and check-in feature is enabled and the corresponding icons are displayed on the detail page of a file. This is the default setting value.
- **false** - the file check-out and check-in feature is disabled and the corresponding icons are hidden.

Configure the sort order of object list views by modification date

Use the **Sort by Modification Date** setting to globally configure the sorting behavior of objects in list views so that objects are listed by their modification date. By default, objects in a list view are listed by name.

For example, an object type has multiple associated objects. By default, associated objects are listed by name in a list pane on a Detail View page. However, users want to see associated objects that are listed by their last modified date. To globally change the sort order of objects in list panes so that objects are listed by the date they were last modified, you would set the value of the **Sort by Modification Date** setting to **true**.

Applications > GRCM > List View > Sort by Modification Date

Default: false

Values:

- **true** - objects in a list view are sorted by their last modification date.
- **false** - objects in a list view are sorted by name. This is the default setting value.

Modify the deletion interval for a reporting period

You can configure the number of days in which a reporting period can be deleted after it is created. After the specified interval, the reporting period can no longer be deleted.

Applications > GRCM > Reporting Periods > Delete Interval

Default: 7 days

Value: In the **Value** box, edit the number of days you want for the deletion interval.

Show hidden settings

Some settings are hidden to protect these settings from being modified. To display hidden settings, change the value in the **Show Hidden Settings** setting.

Applications > Common > Configuration

Default: false

Values:

- **true** - show hidden settings.

- **false** - hide hidden settings.

Specify the browsers that can access IBM OpenPages

You can specify which browsers can be used to access IBM OpenPages with Watson by configuring a list of allowable browsers. All browsers that are not in the list are blocked.

To use the **Allowed Browsers** setting, do the following steps:

1. Ensure that the following settings are enabled (set to **true**):
 - **Platform > Security > Cross-site Scripting Filter**
 - **Platform > Security > Advanced XSS Filter**
2. Configure the **Allowed Browsers** setting. For more information, see [“Allowed Browsers setting”](#) on page 603.
3. Add the following environment property to the <OP_HOME>/aurora/conf/aurora.properties file.

```
enforce.browser.support=true
```

4. Restart the OpenPages application servers.

To disable this feature, set the `enforce.browser.support` environment property to **false** and then restart the OpenPages application servers.

Allowed Browsers setting

Applications > Common > Configuration > Allowed Browsers

Default: Empty, all browsers are allowed to access OpenPages

Values: A list of allowed browsers.

Type a pipe (|) delimited list of browsers that users can use to access OpenPages. The delimited list can specify browsers in general or specific versions of a particular browser.

To allow Microsoft Edge Chromium, type `Edg` (without the `e` on the end).

To specify a particular browser version, you need to know the User-Agent value for the browser that you want to add to the list. For example, for Microsoft browsers, see <https://docs.microsoft.com/en-us/microsoft-edge/web-platform/user-agent-string>.

Example: Allow Microsoft Edge Chromium and Google Chrome.

```
Edg | Chrome
```

User provisioning settings

Administrators can configure the behavior of the Create User wizard and the Users page with the following settings.

To access the user provisioning settings menu items, you must have the Settings application permission set on your account.

Copy Access From Inactive

Determines whether inactive users can be the source for the Copy Access From operation.

Applications > Common > Administration > User Provisioning > Copy Access From Inactive

Default: **true**

Values:

- **true** - allows you to select inactive users to copy access from.
- **false** - inactive users cannot be selected to copy access from.

Copy User Info Attributes

Determines the default behavior for the Locale, Profiles, Group Memberships, Direct Role Assignments, and Direct Reports Access attributes during the Copy Access From operation. A name=value pair is used for each attribute, such as Locale=Yes. Name=value pairs are separated by a comma.

Applications > Common > Administration > User Provisioning > Copy User Info Attributes

Default: Locale=Yes,Profiles=Yes,Group Memberships=Yes,Direct Role Assignments=Yes,Direct Reports Access=Yes

Values: If a name pair is missing, the copy operation is not available. For example, if Profiles=Yes is not listed in the **Value** box, profiles are not copied during the copy operation.

- **Yes** - by default, the attribute is copied.
- **No** - by default, the attribute is not copied. If a name=value pair is missing, No is assumed. For example, if Profiles=Yes is not listed in the Value box, profiles are not copied by the copy operation.
- **Not available** - the attribute cannot be copied.
- blank - if the **Value** box is empty, the Copy Access From operation is not available.

Copy User Info Choice

Determines whether the Copy Access From operation adds to or replaces a user or group's existing attributes.

Applications > Common > Administration > User Provisioning > Copy User Info Choice

Default: Replace

Values:

- **Replace** - existing attributes are overwritten by the Copy Access From operation.
- **Add** - new attributes are merged with existing ones and duplicates are removed. No validation is done after the merge to ensure that there are no conflicts.
- **Choice** - means you can choose between Add or Replace each time that you do a Copy Access From operation.
- **Not Available** - you cannot perform the Copy Access From operation.

Default Allowed Profiles

Determines the default value or values for the Allowed Profiles.

Applications > Common > Administration > User Provisioning > Default Allowed Profiles

Default: blank

Values: Possible values are any profiles in the system. Use a dollar sign and semicolon (\$) to separate profile names in the list. If the value is blank, the Default Profile is used as the Allowed Profile.

Note: Disabled profiles cannot be used as an Allowed Profile, even if they are included in this list.

Default User Change Password

Determines the default change password behavior when you create a new user.

Applications > Common > Administration > User Provisioning > Default User Change Password

Default: blank

Values:

- blank - if the **Value** box is empty, the password expires in 90 days, and the user can change the password then.
- **cannot** - user cannot change password. Using this value forces **Password never expires**, and ignore the **Default User Password Expiration** setting.
- **must** - user must change password at next login.

Default User Password Expiration

Determines the default password expiration behavior.

Applications > Common > Administration > User Provisioning > Default User Password Expiration

Default: blank

Values:

- blank - password expires in 90 days.
- n - password expires in n days, where n is an integer in the range 1 - 99.
- **never** - password never expires

New User Default Locale

Determines the default value for the locale.

Applications > Common > Administration > User Provisioning > New User Default Locale

Default: en_US

Values: Allowed values are any of the OpenPages supported locale codes, such as de_DE, en_US, and it_IT.

Reports Access Page Size

Determines the number of rows that are listed per page in the Reports Access table.

Applications > Common > Administration > User Provisioning > Reports Access Page Size

Default: 20

Values: In the **Value** box, type a positive integer. If the number of rows is less than this number, there is no paging.

Users Can Copy Access From

Determines which users can be used as source for the Copy Access From operation.

Applications > Common > Administration > User Provisioning > Users Can Copy Access From

Default: blank

Values: In the **Value** field, type a comma-separated list of users that can be used as source for the Copy Access From operation. If the value is blank, no users can be used as source for the copy operation. A value of **\$ALL\$** means that any user can be used as source. Use the **Copy Access From Inactive** setting to determine whether inactive users can be used. For more information, see [“Copy Access From Inactive” on page 603](#).

Configure actor table page size

Use the **Page Size** setting to control the number of rows that are listed per page. This setting applies to the following administrative areas within the IBM OpenPages with Watson application: user and group management, role assignments, profile user association, and custom security.

Applications > Common > Administration > Users and Groups > Page Size

Default: 100

Values: In the **Value** box, type a number.

Actor selectors: Configure the bucket size of the phonebook

You can use the **Bucket Size** setting to control the number of user names that are displayed in a bucket or category within the User Selector phonebook style pop-up dialog box.

For information about the phonebook, see [“Modifying the phonebook” on page 358](#).

The number of buckets that are displayed in the phonebook is determined by the size of the bucket and the number of users. For example, if there are 100 users and the bucket size is set to 20, the phonebook would display 5 buckets of 20 users per bucket.

Applications > Common > User Selector > Bucket Size

Default: 10

Values: In the **Value** box, type a numeric value for the number of users you want displayed per bucket.

Actor selectors: Configure display columns in a selector dialog box

For all selector display types, you can use the **Fields** setting to configure additional display information for users and groups.

This setting applies when a phonebook style user or group selector dialog box is open on certain pages, including when:

- assigning a user or group administrator permissions from a Security Domain page
- selecting the starting group when configuring display type attributes for a user or group field in a profile

For information about selector dialog boxes, see the topic [“Modifying the selector dialog box”](#) on page 358.

Note:

- The **Name** column is always displayed as the first column of the table and cannot be removed or changed. The **Name** column in a User Selector represents the user account name (Username). In a **Group** selector, it is the name of the group.
- The values in the setting are globally displayed in the appropriate selector dialog box. For example, if you set the first name of a user to be displayed, the user's first name would appear in the User and User/Group dialog boxes but not the Group dialog box because the Group dialog box lists only groups (no users).

Applications > Common > Actor Selector > Fields

Default: If no values are present in the **Fields** setting, the **Name** and **Description** column headings are displayed by default.

Values: In the **Value** box, type one or more of the following codes in the order in which you want the columns to display in a User, Group, or User/Group Selector dialog box:

Table 194. Column heading display codes		
To display this column heading...	Type this code...	Comments
Description	%DN;	Displays any description information from the "Description" object field on a User or Group Information page. This column heading is displayed by default in the User, Group, and User/Group Selector dialog boxes.
First Name	%FN;	Displays information from the "First name" object field on a User Information page. This column heading is displayed only in the User and User/Group Selector dialog boxes.
Last Name	%LN;	Displays information from the "Last name" object field on a User Information page. This column heading is displayed only in the User and User/Group Selector dialog boxes.
Email	%EM;	Displays the email address of a user from the "Email" object field on a User Information page. This column heading is displayed in the User, Group, and User/Group Selector dialog boxes.

For example, to display the email address of users followed by a description of the user, type the following codes in the **Value** box: %EM;%DN;.

The result of these settings in the User Selector is that the **Name** column is followed by the **Email** and **Description** columns.

Actor selectors: Configure users and group selectors for search

Deprecated.

Applications > GRCM > Detail Page > Use Actor Search Only

Menus: Update administration menus

Customize the administration menus for your users by adding custom menu items.



Attention: Users do not see changes to menus until the next time they log in.

Applications > GRCM > NavigationMenu > Administration > SubItems

Default: none

Values:

For example, *YourCustomMenuItem,Security,Schema,Application,Management*.

Menus: Modify the order of menus

The navigation bar in IBM OpenPages with Watson contains various menus that represent categories for grouping views and object types. Use the **Items** setting to modify the order in which the main menus are displayed on the navigation bar.

Which categories for object types are available as menus on the navigation bar depends on your particular business solution.

Applications > GRCM > NavigationMenu > Items

Default: **My OpenPages** is typically displayed as the first menu item on the navigation bar, and **Administration** as the last menu item.

Values: In the **Value** box, modify the order of the menus as you want these to appear on the navigation bar.

Note:

- The list must be comma delimited.
- The order in which the menus are defined in the list determines the order in which the menus are displayed on the navigation bar in the application user interface.

In the following example, the menus on the navigation bar are displayed as follows: My OpenPages followed by Reports, Organization, Remediation, and then Administration.

```
MyOpenPages,Reports,Organization,Remediation,Administration
```

- The list must not have any leading or trailing spaces.

Changes to menus do not appear until users log out and then log back in to the application.

Menus: Modify submenus

The navigation bar in the IBM OpenPages with Watson application contains various menus that represent categories for grouping views, object types, and system pages.

There are two types of menu items that you can add to a menu: object types (ObjectTypes) and system pages (SubItems).

Applications > NavigationMenu > <folder_name>

Default: none

Values:

Note:

- The list of submenu items must be comma delimited.
- You can use the `__separator__` (two underscores) keyword to organize submenu items into groups.

The following example shows how to create two groupings of object types in a list.

```
RiskAssessment,SOXRisk,__separator__,SOXControl,SOXTest,SOXTestResult
```

The result is a list of submenu items that are grouped as follows:

```
Risk Assessment
Risk
-----
Control
Test
Test Result
```

- The order in which the submenu items are defined in the list determines the order in which the submenu items are displayed in the selected menu on the application user interface.
- The list must not have any leading or trailing spaces.

Menus: Show items on the Administration > Object Menu

Customize the **Object Menu** for your users by showing menu items for specific object types (Standard UI only).

The object types that are listed in this setting are displayed under **Administration > Object Menu** in the Standard UI. To remove an object type from the menu, remove the object type from this setting.

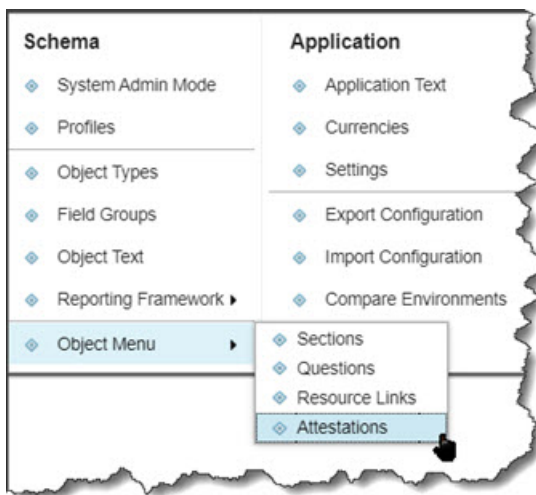


Figure 59. Object Menu

Applications > GRCM > NavigationMenu > Administration > Schema > SpecialObjectTypes > ObjectTypes

Default: none

Values:

Note: The list of object types must be comma delimited.

Object auto-naming settings

For most object types, you can auto-generate their names when they are created or copied. This ability allows users to enforce internal naming policies and ensure unique object names.

The auto-generation of object names is controlled by a series of settings. It is possible to turn autonaming on or off for each object type individually. For example, you might want all business entities and processes to be named by users, but all risks, controls, and test plans named automatically by the IBM OpenPages with Watson application.

Note: Auto-naming is not supported for the following object types: SOXDocument and SOXSignature.

Although auto-naming is not supported for SOXDocument objects, you can control how duplicate file names are handled. For information, see [“SOXDocument object auto-naming settings for duplicate file names” on page 611.](#)

Applications > GRCM > Auto Naming

Default: none

Values: For each object type, you can modify the following settings:

Table 195. Auto-naming settings to modify	
Setting name	Description
Auto-named folder	Flags this folder as using auto-naming.
Copied object	Determines whether or not copied instances of the selected object type are automatically named. If the value is set to: • true - auto-naming is enabled for copied instances. Note: Only the object that is directly selected for copy will be auto-named. Any child objects associated with the selected object will not be renamed, even if the Copied Object setting is set to true for these associated child objects. • false - auto-naming is disabled for copied instances. The default value is false. Auto-naming also applies to new instances of child objects but not to grandchild objects.
New object	Determines whether new instances of the object are automatically named. If the value is set to: • true - auto-naming is enabled for new instances. • false - auto-naming is disabled for new instances. The default value is false.

Table 195. Auto-naming settings to modify (continued)	
Setting name	Description
Can be edited	Determines whether the generated name can be edited during the creation process. If the value is set to: • true - the generated name can be edited. • false - the generated name cannot be edited. The default value depends on the object type.
Default parent name	If the created object has no parent, the value for this parameter will be used to replace the "%P;" variable in the generated name.
Format	Determines the format of the generated name. Additional details can be found in “Configure the format of object names” on page 610 .

Configure the format of object names

The **Format** setting allows you to incorporate some contextual information about the object, as well as an identifier in the object name.

You can use the variables that are described in the following table to format the auto-generated name.

Applications > GRCM > Auto Naming

Default: none

Values:

- In addition to the variables, you can include any valid text in the auto name.
- The name of an object:
 - Must be 252 bytes or less.
 - Cannot contain forward slashes (/), backslashes (\), or the ellipsis character (...).
 - Must contain either the %Nn or the %Rn token.

Table 196. Auto-naming variables	
Variable	Meaning
%P;	Will be replaced with the name of the parent of the new object. If the created object has no parent, the value of the default setting will be used.
%U;	Will be replaced with the creator's user name.
%Nn;	A unique sequentially generated numeric identifier. Where: n" specifies the amount of padding the number has. For example, %N3 might result in 001, 002, 003, while %N5 might result in 00001, 00002, 00003, and so forth.
%Rn; [5.5.1 added - OPX]	A unique randomly generated alphanumeric identifier. Where: n" specifies the amount of padding the number has. For example, %R3 might result in T6d, while %N5 might result in T6d3fF, and so forth.

Name examples

If we use a parent Process of "Hiring Practices" and a creator of "JSmith", and have the following settings:

- **Auto-Named** value is set to **true**
- **Can be Edited** value is set to **false**
- **Format** value is set to **%P;_RIS_%N7;**
- **Default Parent Name** has no value set.

The auto-generated name is "Hiring Practices_RIS_0000001" and could not be edited.

Example 1:

For the auto-naming format parameter

```
Format is set to:%P;-Risk-%N5;
```

the generated Risk name is "Hiring Practices-Risk-00001".

Example 2:

Given a different auto-naming format parameter, such as

```
Format is set to: Risk %N3; for %P; (%U;)
```

would result in the generated name "Risk 001 for Hiring Practices (JSmith)"

Example 3:

Not all of the variables need to be used in an auto-generated name. For example,

```
Format is set to: Risk %N4;
```

results in "Risk 0001"

Example 4:

If the risk had no parent process, the value of **Default Parent Name** is used. In this case, the value

```
Format is set to: %P;_RIS_%N7;
```

results in "_RIS_0000001"

SOXDocument object auto-naming settings for duplicate file names

Use the Auto Remediate Duplicate File Names setting to control auto-naming for SOXDocument objects.

Within a folder, file names for SOXDocument objects must be unique. This setting controls what happens when a duplicate file name is added. The system can add a numeric suffix to the file name or force the user to rename it.

Applications > GRCM > Auto Naming > SOXDocument > Auto Remediate Duplicate File Names

Default: true

Values:

- **true** - adds a numeric suffix to the file name.
- **false** - forces users to rename the file.

In infrequent user applications, such as questionnaire assessments and IBM OpenPages Loss Event Entry, this setting is ignored and duplicate file names are automatically renamed.

In Folder View, this setting is ignored and an error is issued when a user saves a duplicate file name in the folder. The user must manually rename the file.

Environment migration settings

If your organization has multiple IBM OpenPages with Watson environments, you can move data from one environment to another without needing physical access to either environment. Migration means exporting from a source environment and importing into a target environment. You can use settings to configure the environment migration tools.

Applications > GRCM > Environment Migration

For more information, see [“Settings that apply to environment migration” on page 865.](#)

Report fragment settings

For all profiles, you can globally configure the size of the pop-up window for report fragment fields in certain object views.

A report fragment pop-up window can be sized:

- Manually - by specifying the size of the pop-up on the field definition page of a report fragment field.
- Automatically - if no size is specified on the field definition page of a report fragment field, the pop-up window will be automatically sized using the settings in [Table 197 on page 612.](#)

Report fragment fields with a display type of On Demand always display Cognos report components in a pop-up window.

For report fragment fields with a display type of 'Automatic', the display behavior varies depending on the object view:

- For Detail and/or Activity View pages - Cognos report components are always embedded directly into the cell of the report fragment field.
- For view pages that have a tabular format, such as List View, Folder View, and Filtered List View pages, and on the My Work tab on the Home page - Cognos report components are displayed in pop-up windows.

The sizing rules for report fragment field pop-up windows apply to both On Demand and Automatic display types used in List and/or Folder Views.

Applications > Common > Report Fragments > Popup

Values: Click one of the settings to open its detail page. In the **Value** box for the selected setting, change the existing value to a new number (must be greater than zero).

<i>Table 197. Settings for reporting fragment pop-up windows</i>		
Setting	Description	Default Value
Maximum Height	Sets the default maximum height allowable for a report fragment pop-up window.	375
Maximum Width	Sets the default maximum width allowable for a report fragment pop-up window.	575
Minimum Height	Sets the default minimum height allowable for a report fragment pop-up window.	250
Minimum Width	Sets the default minimum width allowable for a report fragment pop-up window.	350

Set the mail server address

Use the **Mail Server** setting to configure your mail server so you can automatically send email notifications to users from your JSP-based reports or the Notification Manager utility.

The **Mail Server** setting is also used to do mail routing for objects that use lifecycles, for example, questionnaire assessments and incidents. Email notifications are sent to lifecycle assignees when a lifecycle starts and with every transition except for close transitions.

For emails generated by lifecycle triggers, the sender address is specified in the `trigger.xml` file. The default is `donotreply@openpages.com`. For more information about lifecycle triggers, see the *IBM OpenPages with Watson Solutions Guide*.

Depending on your environment, you can configure the following settings:

- SMTP Password
- SMTP Port
- SMTP Security Type
- SMTP User Name
- SOCKS Proxy Private IP Address

Define SMTP Port and SMTP Security Type if you use a third-party SMTP provider. Valid values for SMTP Security Type are SSL/TLS and STARTTLS. You must also import the SSL certificate from the SMTP server provider. Refer to the SMTP provider's documentation and import it by using `keytool`. Leave SMTP Port and SMTP Security Type empty if you have an unencrypted connection that uses the default port number. In this case, the SMTP servers are behind a firewall and a third-party SMTP provider is typically not used.

Some settings might be hidden. For information about unhiding settings, see [“Show hidden settings” on page 602](#).

Note: Override this global setting by entering the name of a mail server in the notification Mail Server parameter.

Applications > Common > Email

Default: `mail.yourcompany.com`

Values: In the **Value** box, enter the values for **Mail Server**, **SMTP Password**, **SMTP User Name**, and **SOCKS Proxy Private IP Address**, as required by your mail system.

In **Mail Server** enter a fully qualified server host name, for example, `mail.openpages.com`.

For more information if you have legacy or older JSP reports and want to send email notifications to users from these legacy JSP-based reports or the Notification Manager utility, go to [“Configure self-contained object types” on page 636](#).

Optimize file uploads

To enhance the performance of large files for upload to the IBM OpenPages with Watson Standard UI, you can enable the **Optimized File Upload** setting. This setting applies only to Microsoft Internet Explorer 11.

The **Optimized File Upload** setting applies to uploading files in the Standard UI. It does not apply when uploading files in the Task Focused UI.

You can optimize the upload only if you are using the **Edit/Upload this File** option. You cannot optimize the upload if you use the **Add New** option.

When enabled, this feature provides the following functions:

- Compresses the selected file on the user machine before uploading it to the OpenPages with Watson repository.
- Displays additional Optimized File Upload text and a **Browse and Save** icon to users for attaching files.

Note:

- The file upload applet requires the Java Runtime Environment (latest version) on the client browser.

- When using the Chrome browser, if the registry setting **Applications > Common > Optimized File Upload** is set to `true`, the setting is ignored by the Chrome browser.

By default, this value is disabled.

Applications > Common > Optimized File Upload

Default: `false`

Values: In the **Value** box, type `true` or `false`

- `true` - The Optimized File Upload **Browse and Save** icon is displayed to users in addition to the standard file upload icon.
- `false` - Only the standard file upload icon is displayed to users.

Number of objects in listing pane

Use the **Page Size** setting to control the maximum number of associated objects that can be listed in a child object listing pane on Detail View and Activity View pages.

Applications > GRCM > List View > Page Size

Default: 20

Values: In the **Value** box, type a number greater than zero.

If the number of child objects that are returned exceed the set value, a Rev and Next link is displayed.

Set copy operations

You can configure settings in the **Copy Options** folder to resolve duplicate names during copy operations and show additional copy options to users during a Copy From operation.

Note:

- During a copy operation for self-contained objects, if a naming conflict exists between the source and the target object, the copy operation will fail and the naming conflict resolution choices made by a user are ignored (see [“Configure self-contained object types”](#) on page 636).
- Self-contained object types and security context point object types do not respect the "copyof" naming option, if selected. By definition self-contained and security context point objects types automatically have their own folder, so no Copy Of prefix is required.
- In a Copy From operation, the target folder path is based on the closest self-contained parent object.

Table 198. Copy Operations Configuration Settings

Setting	Description
Conflict Policy	Set the default behavior of the copy operation when it encounters a duplicate object name during a copy operation. If the value is set to: • overwrite - a new version of the object in the target directory is created with all of the information of the copied object. All prior versions of the object in the target directory are maintained. • copyof - during the copy operation, any objects with the same name as an existing object in the target location will be renamed to "Copy of <objectname>". Note: Consider carefully whether to use overwrite or copyof when you copy objects that have the same name coming from different hierarchies. The end result if you use overwrite will be a single object with many versions. However, if you use copyof, it will be many objects with one version. • existing - if a copied object has the same name as an object in the target location, that file will not be copied. All other objects (without duplicate names) will still be copied to the target location. If you choose this option, you should examine the results of copy operations to determine whether any associations between objects have changed as a result of the copy. For example, if an associated risk is not copied to the new location because an existing risk has the same name, the copied parent process of the risk will be associated with the pre-existing risk in the target location. The default value is overwrite.
Max Object Trees Copied Interactive	This setting is a positive integer that determines when the copied objects are created. If the user chooses to copy the objects and their descendants, and the number of selected objects is less than or equal to the value of this setting, the dialog stays open until the copies are complete, blocking other actions. If the number of selected objects is greater than the value of this setting, then the copies are created in the background. The user receives an email when the copy process has completed. The default value is 20.
Max Top-level Objects Copied Interactive	This setting is a positive integer which determines when the copied objects are created. If the user chooses to only copy the objects themselves without any descendants, and the number of objects to be copied is less than or equal to the value of this setting, then the copies are created while the user waits. If the number of objects to be copied is greater than the value of this setting, then the copies are created in the background. The user receives an email when the copy process has completed. The default value is 250.

Table 198. Copy Operations Configuration Settings (continued)	
Setting	Description
Show Copy Options Page	This setting is only used when the Use Legacy Copy option is true. Allow users to select how duplicate names will be handled for the current copy. This setting displays the following options to users during a copy operation: • <i>Create a new version of the existing object in the destination directory.</i> This is the default selection. This option corresponds to the "overwrite" value in the Conflict Policy setting. • <i>Create new object whose name is prefixed with "Copy Of".</i> This option corresponds to the "copyof" value in the Conflict Policy setting. • <i>Do not copy resources with naming conflicts.</i> This option corresponds to the "existing" value in the Conflict Policy setting. If the value is set to: • true - the additional copy options are displayed to users. • false - no additional copy options are displayed to users. The default value is false.
Show Name Conflict Resolution Options	Specifies whether to display the name conflict resolution options in the Copy Wizard options tab. If the options are not displayed to the user, the value from the Conflict Policy setting is used. The default value is true.
Show Object Copy Options	If this value is set to true, the user is allowed additional control of what is copied with the selected objects. Users are able to choose if just the objects themselves are copied, or if descendants of the object are copied as well. By default, descendants are copied as well. Even if they choose to copy descendants, by default files and issues are not copied. If this option is set to true, users have the opportunity to also include files and issues. The default value is true.
Use Legacy Copy	Controls whether the copy operation uses the new interface or the legacy interface. Permissible values are true or false.

Date field display format

The **Date field display format** setting controls how date fields are displayed for GRC objects. It does not affect dates that appear in other areas of the system. It affects only how date fields are displayed and not the format when users enter date values.

The **Date field display format** setting and the locale determine how date fields are displayed. The examples below illustrate how the date, October 25, 2016, is displayed given different date formats and locales:

Table 199. Date field display format		
Locale	Date field display format	Result
US English	SHORT	10/25/16
US English	MEDIUM	Oct 25, 2016
US English	LONG	October 25, 2016

Table 199. Date field display format (continued)

Locale	Date field display format	Result
UK English	SHORT	25/10/16
UK English	MEDIUM	25-Oct-2016
UK English	LONG	25 October 2016
Simplified Chinese	SHORT	16-10-25
Simplified Chinese	MEDIUM	2016-10-25
Simplified Chinese	LONG	2016年10月25日

Applications > GRCM > Date Field Display Format

Default:

The values are:

- **short** - dates are displayed in Java Locale SHORT format.
- **medium** - dates are displayed in Java Locale MEDIUM format.
- **long** - dates are displayed in Java Locale LONG format.

Configuring large files for upload

By default, the maximum upload size for files in IBM OpenPages with Watson is 250 MB. If you have files that are larger than this limit, you can configure the system to upload larger files. Files greater than 2 GB are not supported.

Procedure

1. Log on to the Task Focused UI as a user with administrative privileges.
2. Click  > **System Configuration > Settings**.
3. Click **Applications > Common > Max File Upload Size**
4. In the **Value** field, type the maximum upload size as a numeric value followed by a single letter to represent the unit. For example: 200K, 500M or 1G.
5. Click **Done**.
6. Restart the OpenPages with Watson application service.

For details on starting services, see [Chapter 24, "Starting and stopping servers," on page 841](#).

Allow opening Microsoft Office files directly from OpenPages

You can configure whether users can open and edit Microsoft Office files directly from OpenPages (Task Focused UI only).

Before you begin

Verify that Microsoft Office 2016 or Microsoft 365 is installed locally for users.

Verify that SSL is enabled.

Test that users can open Microsoft Office files from OpenPages.

If the OpenPages application server is using a self signed certificate, end users must import the certificate into the trust store on their local computer. Otherwise, a blank screen is displayed when they try to open a Microsoft Office document from within OpenPages. This type of certificate might be used in certain situations, for example, in a test environment.

1. Click the lock icon in the browser URL (Chrome).
2. Click Certificate.
3. Click the Details tab and click Copy to File (to export the certificate).
4. Click Next and accept all defaults.
5. Enter a file name and click Finish.
6. From the Control Panel, type Manage User certificates to open the *certmgr* tool.
7. Click Trusted Root Certificates > All Tasks > Import (to import the certificate you just saved).
8. Close the browser.
9. Open a new browser session.

About this task

The functionality of this feature is similar to inline editing. Users can open Microsoft Office files directly from OpenPages. Every time a user clicks save within a file that is opened in this way, the file is saved in the OpenPages file repository. However, other users cannot see the changes until the file is checked in.

If enabled, users can open and edit Microsoft Office files from the following access points in the Task Focused UI:

- In a Task View for an object type, where the Task View contains a Grid relationship field for the File object type.
- In a Task View for the File object type.

The feature is available:

- Only on Microsoft Windows clients. It is not available on Mac operating systems.
- Only if Microsoft Office 2016 or Microsoft 365 are installed locally for users.
- Only for Word, Excel, and PowerPoint files with the following extensions: .doc, .docx, .xls, .xlsx, ppt, pptx.
- Only if the OpenPages URL has an HTTPS protocol, not HTTP.

The  (View) and  (Edit) icons are displayed in a Task View if the following conditions are met:

- The feature is enabled.
- The  (View) icon is displayed if the user has read access rights to the file.
- The  (Edit) icon is displayed if the user has write access rights to the file and if no other users have the file checked out.
- Both icons are not displayed in rows for all other file types, for example, PDF files and text files.

Procedure

1. Log on to the Task Focused UI as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Applications** > **Common** > **Configuration** > **Disable opening files with MS Office desktop**.
4. In the **Value** field, type a value:
 - False - editing is enabled (users can open and edit Microsoft Office files directly from OpenPages). This is the default.
 - True - editing is disabled (users cannot open and edit Microsoft Office files directly from OpenPages).
5. Click **Done**.

Reviewing the Net Promoter Score (NPS) survey settings

The **Applications > NPS > Embedded Survey URLs** setting is part of the integration between a Net Promoter Score survey provider and OpenPages.

About this task

OpenPages provides a default URL value that should not be changed except on the advice of IBM OpenPages Support.

Procedure

1. Log on to the Task Focused UI as a user with administrative privileges.
2. Click  > **System Configuration > Settings**.
3. Click **Applications > NPS > Embedded Survey URLs**.
4. In the **Value** field, review the URL of the embedded NPS survey provider.
5. Click **Done**.

What to do next

Complete the remaining steps to configure a Net Promoter Score survey. For more information, see [“Configuring a Net Promoter Score \(NPS\) survey”](#) on page 450.

Signature and lock settings

IBM OpenPages with Watson allows users to create "signatures" on objects. A signature is a note that signifies the user agreement that the object meets with the user approval. It has no enforcement powers, and does not prevent the item from being modified after approval is given.

A signature lock is a lock that is placed on an object and its descendants. It prevents the objects from being modified. The lock is activated by placing a signature on an object. After the signature is added, the lock is active. The signed object and all of its associated child objects in the object hierarchy cannot be modified until the signature is revoked or an administrator removes the lock.

Only one active lock can be placed on an object. Multiple locks can be inherited from parent objects as those objects are locked.

All of the following actions are accessed from the Applications folder.

To access the registry settings, you must have the Settings application permission set on your account.

Signatures

Signatures are added on the Detail page of an object type by clicking the **Signatures** field. If configured, users can add, edit, and revoke signatures for the specified object type from the **Actions** menu on the **Signature** pane.

The **Actions** menu is hidden from users who do not have the correct permissions.

When you configure signatures for a specific object type (such as **Processes** or **Accounts**), you grant permission to a group of users to add a signature. The group is able to add, edit, or revoke a signature for the specified object types to which they have Read access.

To enable a user group to add or revoke signatures directly on an object, you must configure the **Permission** setting for the specified object type. For details, see [“Configure signatures”](#) on page 619.

Configure signatures

When you add a group to an object type setting for signatures, sign-off is enabled for objects of that type. Users who belong to the group can add and revoke signatures. Click **Actions** on the **Signatures** pane to add a signature to the object type.

Note: Only groups that are defined in object type can sign off on objects of that type. Sub groups of a group do not inherit the sign-off permission.

Applications > GRCM > Signature > Permission

Default: enabled

Values: In the **Value** box on the setting detail page, complete the following steps:

- To configure groups to add a signature to an object type, type the name of the group to add.

Note: If you are entering multiple user groups, use a comma to separate group names, and do not use a space after the comma.

For example, to add the groups Auditors and Managers to the sign-off list for Process object types, the value in the SOXProcess setting is defined as follows: **Auditors,Managers**

- To disable one or more user groups from adding a signature to the selected object type, delete the group name.

Configure signature locks

The **Mode** setting controls whether a lock is created when a signature is added. When the Autolock value is set, adding a signature to an object creates a lock on the object. It prevents further changes to the object and any object that is associated with it. Revoking a signature removes the associated lock.

Note: When the locking feature is enabled, users can create signatures only on items to which they have Write privileges.

Applications > GRCM > Signature > Mode

Default: none

Values: In the **Value** field, type one of the following values:

Table 200. Lock values	
Value	Action
None	No lock is applied to the object when a signature is added.
Autolock	The object is locked when a signature is added. Only users with Write permission for an object can create a signature.
Cascade	Cascading signatures as specified in the Cascade setting are enabled for child objects (for details see, “Configure signatures” on page 619).

Configure the signature status field

The OPSS-Sig:Status field contains enumerated values for signature status.

About this task

The OPSS-Sig:Status field is by default a single-value enumerated field with two values: *In Effect* or *Revoked*.

An issue exists in that if you change OPSS-Sig:Status to a multi-valued enumerated field, signatures can no longer be created.

A workaround for this issue is to set the **Applications > GRCM > Special Object Fields > SOXSignature Status Field** registry setting to OPSS-Sig.Status.In Effect.

When **Applications > GRCM > Special Object Fields > SOXSignature Status Field** is set to **OPSS-Sig.Status.In Effect**, signatures can be created. Signatures can also be revoked but only when a Chrome browser is used.

Configure cascading signatures

When a signature is added to a parent object, you can automatically apply signatures to all associated objects in the hierarchy, below the signed object. For example, signing a process applies the signature to any sub processes, accounts, risks, controls, and tests that are associated with the process.

This feature is turned off by default. It is enabled through the **Cascade** setting.

Note: To enable cascading signatures, the **Mode** setting must have the **Cascade** value set (for details see, [“Configure signature locks” on page 620](#)).

> GRCM > Signature > Cascade > <object>

Default: none

Values: In the **Value** box on the setting detail page, complete the following steps:

- To add a cascading signature to child objects, type the name of the child object type.

Note: If you are entering multiple child objects, use a comma to separate the names, and do not use a space after the comma.

For example, to add a cascading signature to the Process object type for child sub-processes, accounts, and risks, the value in the SOXProcess is set to the following value:

SOXSubprocess,SOXAccount,SOXRisk

- To remove a cascading signature from child objects, delete the name of the child object type.

Lock and unlock objects

Locks can be applied to objects without the use of signatures.

Users lock entire object hierarchies by adding a signature, if Autolock is enabled, or by selecting **Lock this** on the Actions menu of an detail page.

The **Lock** and **Unlock** application permissions control whether users can lock and unlock objects. For details, see [“Configure the Lock and Unlock application permissions ” on page 621](#).

Note: Unlocking an object using the **Actions > Unlock this** menu item does NOT revoke the signature.

For information about globally unlocking business entities, see [“Globally unlock business entities” on page 623](#).

Access privileges for locking

By default, "Read" permission is required to lock an object. This setting can now be configured through a property in the *aurora.properties* file named "allow.locking.read.access". This property is set to false by default.

When set to 'true', users with Read access to an object can lock the object by adding a signature. The default value of false requires that users have at least "Write" access to an object before they are allowed to lock it.

Configure the Lock and Unlock application permissions

The **Lock** and **Unlock** application permissions control whether users can lock and unlock objects.

The **Lock** application permission allows a user to lock any unlocked object, as long as the user has Write permission to the object and all associated objects down the hierarchy.

The **Unlock** application permission allows a user to unlock any locked object, as long as the user has Write permission to the object and all associated objects down the hierarchy.

You assign application permissions either to a role template or to a user group that a user belongs to.

- On a role template, the **Lock** and **Unlock** application permissions are defined in:
 - **Administration > Role Template > <role template> > Role Permissions > Files > Lock**
 - **Administration > Role Template > <role template> > Role Permissions > Files > Unlock**
- On a user group, the **Lock** and **Unlock** application permissions are defined in:
 - **Administration > Users, Groups and Domains > <group> > Permissions > Files > Lock**
 - **Administration > Users, Groups and Domains > <group> > Permissions > Files > Unlock**

For more information, see [“Defining application permissions”](#) on page 90.

Configure the Lock menu item/lock icons for object types

The **Display Lock Button** setting controls by object type whether lock/unlock menu items and icons are displayed.

In the Standard UI, the **Display Lock Button** setting applies to manual and automatic signature locking. The setting controls whether the **Lock this** menu item on the **Actions** menu of an object type is displayed. The user must be assigned the **Lock** application permission for the menu item to display. For details, see [“Configure the Lock and Unlock application permissions”](#) on page 621.

In the Task Focused UI, the **Display Lock Button** setting controls whether the lock and unlock icons are displayed in Grid views for an object type. The user must be assigned the **Lock** application permission for the lock icon to display. The user must be assigned the **Unlock** application permission for the unlock icon to display. For details, see [“Configure the Lock and Unlock application permissions”](#) on page 621.

Applications > GRCM > Locks > Display Lock Button

Default: none

Values:

- To add an object type, type the name of the object type that is separated by a comma.
For example: SOXBusEntity, SOXAccount, SOXSubaccount, SOXProcess, SOXSubprocess, SOXControlObjective, SOXRisk, SOXControl, SOXTest, SOXTestResult, SOXSignature, SOXIssue, SOXTask, SOXDocument, SOXExternalDocument.
- To remove an object type, delete the name of the object type from the list.

Lock child objects when a parent is locked

You can use the object type settings under the **Lock Child Types** folder to configure locks on child objects when a parent object is locked.

For example, you want to lock child Process objects whenever a business entity is locked. You would enter SOXProcess in the setting Value box for SOXBusEntity. When a business entity is locked, users would not be able to add, associate, copy, and disassociate processes to the locked business entity. The child objects of that process will not inherit any locks. If you want to lock its child objects too, then you would have to specify those object types in the value of the SOXBusEntity setting.

Applications > GRCM > Locked Objects > Lock Child Types

Default: none

Values: In the **Value** box of the selected setting, enter the exact name of one or more child object types that should be locked when the parent object is locked.

Find the exact object name listed under the **Allowed Associations** folder.

Note: If there are multiple child object types, you must add a comma to separate each object name. For example: SOXProcess, SOXControl, SOXIssue, SOXDocument, SOXExternalDocument, SOXSignature

Enable icons on locked associated objects

You can enable associations of child objects, such as Risks or Controls, to their locked parent objects. You can define these child objects in the **Allowed Associations** setting. Specifically, the **Add New**, **Associate**, **Copy From**, and **Disassociate** icons or menu items remain available to users on specific Associated object tabs of the parent object, as well as in the detail pages of the child objects.

For example, you can enable the SOXProcess and LossEvent child objects for SOXBusEntity so users can associate processes and loss events to a locked business entity. When enabled, the business entity detail page displays the Associate icons (Add New, Associate, Copy From, and Disassociate) *only* on the Processes and Loss Events tabs. Note that the Associate icons also display on the SOXProcess and LossEvent detail pages.

Configure the registry to enable associations of child objects

You can make objects available to users for association when a parent object is locked.

For object types that are defined in the **Allowed Associations** setting, the **Add New**, **Associate**, **Copy From**, and **Disassociate** actions are enabled and **Delete** is disabled.

For object types that are not defined in the **Allowed Associations** setting, the **Add New**, **Associate**, **Copy From**, **Disassociate**, and **Delete** actions are disabled.

Applications > GRCM > Locked Objects > Allowed Associations

Default: none

Values: In the **Value** field, type the exact name of one or more child object types.

Find the object name listed under the **Allowed Associations** folder (for example, SOXBusEntity).

Note: If you have multiple object types, add a comma to separate each object type name.

When a Business Entity is locked, users can add, associate, copy, and disassociate processes to the locked Business Entity.

Note: The **Disassociation** action is not enabled on a detail page until you select the object you want to disassociate.

Globally unlock business entities

Administrators can enable a global unlock operation for business entities or sub-entities by enabling the **Remove All Tree Locks** application permission for designated groups of users. The Unlock All operation removes all direct and inherited locks on a business entity, including all of its children.

Note: When you enable the **Remove All Tree Locks** application permission for a group, the **Unlock All** icon is displayed only on a business entity or sub-entity detail page.

Typically, you would use the Unlock All operation if

- The remove locks option was not selected after a finalized reporting period.
- Different business sub-entities of a multi-national organization have different reporting-period closure dates during the year. One sub-entity may need to remain locked while other entities are unlocked.

For example:

BE-US is a business entity representing the corporate office of a multi-national firm. BE-IND and BE-UK are two sub-entities within the BE-US entity. December is the financial closure period for BE-UK while March is the closure period for BE-IND.

When BE-US is signed off in December, BE-IND and BE-UK remain locked along with their associated objects. Since December is the reporting-period closure date for BE-UK also, its reporting period is

finalized. If the Unlock All operation is applied to BE-UK exclusively, users can keep working in the BE-UK object hierarchy while BE-IND and its hierarchy remain locked.

Procedure

1. Click  > **Users and Security** > **Domains & Groups**.
2. Click **Groups**.
3. Select **Workflow, Reporting and Others**.
4. Add a new group or select a group and navigate to its **Permissions** section.
5. In the **Permissions** section, click **Edit**.
6. Under **Files**, select **Remove All Tree Locks**.

Object Reset settings

Before performing an object reset, you can set the logging level, whether or not the Reset session should continue or halt if errors are encountered, if ACLs should be checked, and if locks are ignored. These settings need to be set only once, before your first time initiating an object reset, but you may want to change them for different entity trees or ruleset behavior.

Changing the logging level

The **Logging Level** setting controls how much information is displayed on the user interface. The session log captures detailed information regardless of the user interface display setting. You can change the logging information that is displayed on the user interface for a reporting period.

Applications > Common > Object Reset > Logging Level

Default: high

Values:

- low - Only error messages are displayed.
- medium - Both error and warning messages are displayed.
- high - Errors, warnings, and informational or diagnostic messages are displayed.

Continuing on error

The **Continue on Error** setting determines whether the object reset session will log errors and continue to run, or whether the errors will be logged and the session halted. You can change whether the object reset session runs or halts processing when an error is encountered.

Applications > Common > Object Reset > Continue on Error

Default: true

Values:

- true - Errors are logged and processing continues.
- false - Errors are logged and processing is halted.

Obeying ACL restrictions

The **Check ACL** setting controls whether the object reset occurs against all objects contained within the scope of the reset session, or whether the object reset occurs against only those objects to which the user who initiated the reset has access. You can change the scope of the object reset session.

Applications > Common > Object Reset > Check ACL

Default: true

Values:

- true - Includes all objects within the scope of the reset session.
- false - Includes only those objects within the reset session to which the user has access.

Obeying locking restrictions

The **Ignore Locks** setting controls whether existing locks on objects are honored or ignored when running an object reset. You can change whether locks are ignored during an object reset session.

Applications > Common > Object Reset > Ignore Locks

Default: false

Values:

- **true** - Locks on objects will be ignored when running the reset session.
- **false** - Locked objects will not be modified by the reset session.

Home page settings

For profiles, you can globally configure the display of predefined tables, the number of embedded reports, the number of objects in a table, and the number of report listings.

For configured home page filtered lists, you can set the view definition that determines which fields are displayed, the target view of the **Name** hyperlink, and the target view of the **View Details** hyperlink.

Define target of View Details hyperlink on a home page filtered list

You can use the **Show All Link** setting to specify the FLV or grid view to be used for **View Details** targets on home page filtered lists.

Applications > GRCM > Home Page

Open the profile folder that you want to customize filtered lists for (for example, OpenPages PCM Master), add a new folder, and name the folder with the same name as the filter. Then, add the **Show All Link** setting.

If the settings are not available or the setting values are blank, the profile settings are used.

Tip: If you delete and then add the filtered list back to the home page, or when you add a new filtered list to the home page, the folders and settings for the filtered list are created automatically.

Note: These settings do not apply to the predefined lists on the home page (**My Checked-Out Files** and **My Reports**).

Default: blank

Values: In the **Value** box, type **Filtered List** or the name (not the label) of a specific grid view for the **View Details** target.

Order predefined panes on home page

You can use the **Items** settings to control how predefined panes are displayed on a home page. The order of the items determines the order of the corresponding HTML panes.

You can configure the following **Items** settings:

- A global **Items** setting (**Applications > GRCM > Home Page > Items**)
- Profile-level **Items** settings (**Applications > GRCM > Home Page > <profile> > Items**)

The following rules apply:

- The global **Items** setting defines all possible home page items and their sequence. The default is **myCheckedOutFiles**, **myReports**. If you remove an item from the global **Items** setting, the pane is suppressed for all users regardless of how the profile-level **Items** settings are defined.
- The profile-level **Items** settings define home page items and their sequence for users who belong to the profiles. If you remove an item from a profile-level **Items** setting, the pane is suppressed for all users

who belong to the profile. Items that are not included in the global **Items** setting cannot be included in a profile-level **Items** setting.

- If you reorder the sequence of items in a profile-level **Items** setting, it overrides the global **Items** setting for users who belong to the profile.

The following examples illustrate how the settings work together.

<i>Table 201. Examples of the Items setting at global and profile levels</i>		
If the global Items setting is...	And the profile-level Items setting is...	The result is...
myCheckedOutFiles, myReports	blank	None of the panes display on the specified profile.
myCheckedOutFiles, myReports	myCheckedOutFiles, myReports	myCheckedOutFiles, myReports display for the specified profile.
blank	myCheckedOutFiles, myReports	None of the panes display because the global setting is blank.
myCheckedOutFiles, myReports	myReports, myCheckedOutFiles	Panes are reordered to myReports, myCheckedOutFiles

Applications > GRCM > Home Page > Items

Default: **My Checked-Out Files** (myCheckedOutFiles), **My Reports** (myReports)

Values: In the **Value** field, add, remove, or reorder the items.

Applications > GRCM > Home Page > <profile> > Items

Default: is from the global **Items** setting

Values: In the **Value** field, add, remove, or reorder the items.

Allow users to personalize the My Work home page

You can use the **My Work Home Page Can Be Personalized** setting to globally control whether users are allowed to personalize their My Work home page portlets by determining which portlets appear and in what sequence. The user can only choose to make portlets appear that are configured for display on their home page in their profile.

Applications > GRCM > Home Page > My Work Home Page Can Be Personalized

Default: true

Values:

- true - users are allowed to personalize their My Work home page portlets.
- false - users are not allowed to personalize their My Work home page portlets.

Maximum number of embedded reports on the home page

You can use the **Maximum Embedded Reports** setting to globally change the maximum number of embedded reports that can be configured for a home page.

Applications > GRCM > Home Page > Maximum Embedded Reports

Default: 2

Values: In the **Value** field, type a number greater than zero.

Note: Setting this value too high will negatively impact performance.

Maximum objects allowed in a home page pane

You can use the **Maximum Objects** setting to globally control the maximum number of objects that can be listed for each table (excluding My Reports) on a home page.

Applications > GRCM > Home Page > Maximum Objects

Default: 5

Values: In the **Value** box, type a number greater than zero.

Maximum reports allowed on the home page

You can use the **Maximum Reports Listing** setting to globally control the maximum number of reports that can be listed in the **My Reports** table on a home page.

Applications > GRCM > Home Page > Maximum Reports Listing

Default: 5

Values: In the **Value** box, type a number greater than zero.

Define target of Name hyperlink on a home page filtered list

You can use the **Detail Link** setting to customize the fields that are displayed and specify the detail or activity view to be used for hyperlink targets on home page filtered lists.

Applications > GRCM > Home Page

Open the profile folder that you want to customize filtered lists for (for example, OpenPages PCM Master), add a new folder, and name the folder with the same name as the filter. Then, add the **Detail Link** setting.

If the settings are not available or the setting values are blank, the profile settings are used.

Tip: If you delete and then add the filtered list back to the home page, or when you add a new filtered list to the home page, the folders and settings for the filtered list are created automatically.

Note: These settings do not apply to the predefined lists on the home page (**My Checked-Out Files** and **My Reports**).

Default: blank

Values: In the **Value** box, type Detail for the detail view, or the name (not the label) of an activity view for the hyperlink target.

Define view definition used to determine fields displayed on a home page filtered list

You can use the **Fields** setting to customize the fields that are displayed on home page filtered lists.

Applications > GRCM > Home Page

Open the profile folder that you want to customize filtered lists for (for example, OpenPages PCM Master), add a new folder, and name the folder with the same name as the filter. Then, add the **Fields** setting.

If the settings are not available or the setting values are blank, the profile settings are used.

Tip: If you delete and then add the filtered list back to the home page, or when you add a new filtered list to the home page, the folders and settings for the filtered list are created automatically.

Note: These settings do not apply to the predefined lists on the home page (**My Checked-Out Files** and **My Reports**).

Default: blank

Values: In the **Value** box, type `Detail` or the name (not the label) of a specific activity view to determine which fields are shown.

Define target of View Details hyperlink on a home page filtered list

You can use the **Show All Link** setting to specify the FLV or grid view to be used for **View Details** targets on home page filtered lists.

Applications > GRCM > Home Page

Open the profile folder that you want to customize filtered lists for (for example, OpenPages PCM Master), add a new folder, and name the folder with the same name as the filter. Then, add the **Show All Link** setting.

If the settings are not available or the setting values are blank, the profile settings are used.

Tip: If you delete and then add the filtered list back to the home page, or when you add a new filtered list to the home page, the folders and settings for the filtered list are created automatically.

Note: These settings do not apply to the predefined lists on the home page (**My Checked-Out Files** and **My Reports**).

Default: blank

Values: In the **Value** box, type `Filtered List` or the name (not the label) of a specific grid view for the **View Details** target.

Filtered List View settings

You can globally configure the following Filtered List View page settings.



Attention: If you create a new filter that uses the character % as the value, for example Name Contains %2, the Name Contains value field appears empty after you load the filter: the % character does not appear. However, the filter runs properly.

Note: If you are using the FastMap tool, in addition to configuring export settings on a Filtered List View page, you can also configure FastMap import settings to optimize performance. See [“Modifying export settings to optimize FastMap performance”](#) on page 947 and [“Limiting the rows for import to optimize FastMap performance”](#) on page 947.

Initial results configuration of Filtered List View

Use the **Show All Objects** setting to control whether results are displayed on a **Filtered List View** page the first-time users select an object type. By default, no results are displayed to users until a filter is selected or added.

Applications > GRCM > Filtered List > Show All Objects

Default: false

Values:

- `true` - displays all available results (if any). No filter is applied.
- `false` - no results are displayed until a filter is selected or added.

Note: Users can type the percentage symbol (%) in the **Quick Filter** field then click **Apply** to return all available results.

Advanced filters field configuration for Filtered List View

In the Standard UI, use the **Filter on all fields in profile** setting to control whether the fields in a **Detail View** or in a user profile are available for creating an **Advanced Filter** on a **Filtered List View** page.

For example, you might exclude certain system fields (such as **Creation Date** and **Created by**) and custom fields from a **Detail View** of an object type, but include these fields in the user's profile. If you wanted to make all fields included in the user's profile available for creating an **Advanced Filter**, you would set the value of the **Filter on all fields in profile** setting to `true`.

In the Task Focused UI this setting is ignored.

Applications > GRCM > Filtered List > Filter on all fields in profile

Default: `true`

Values:

- `true` - all fields that are included in the user's profile are available for creating filters.
- `false` - only fields that are included in an object type are available for creating filters. In the Standard UI fields that are included in the **Detail View** are available for creating an **Advanced Filter**.

Maximum number of objects to export to Microsoft Excel on the Filtered List View

Use the **Maximum Export Size** setting to control the maximum number of objects that can be retrieved and exported to Microsoft Excel (in `.xls` format) from a Filtered List View page.

If the number of objects that are being exported exceeds the defined number, then the user is prompted to refine their filter.

Applications > GRCM > Filtered List > Maximum Export Size

Default: 1000

Values: In the **Value** field, type a number greater than zero.

Enable object type and field export choices in the Filtered List View

Use the **Enable Object Type and Field Export Choices** setting to allow users to choose which object types and fields to export.

Applications > GRCM > Filtered List > Enable Object Type and Field Export Choices

Default: `true`

Values:

- `true` - choosing object types and fields to export is enabled.
- `false` - choosing object types and fields to export is disabled.

Exclude object types from exports if they are not in a Filtered List View

Use the **Object Types to Exclude in Export** setting to exclude object types from an export unless they are included in the Filtered List View.

Applications > GRCM > Filtered List > Object Types to Exclude in Export

Default: SOXSignature

Values: In the **Value** field, type a comma-separated list of object type names that you want to exclude. For example, if you want to exclude Risk and Control object types, type: SOXRisk,SOXControl.

For example, suppose that you exclude SOXRisk and SOXControl. When users click **Export** in the Process filtered list view, the **Export** dialog box does not show check boxes for Risks, Controls, or descendants of controls because these object types are not in the Process filtered list view.

Exclude object types in Filtered List Views from export

Use the **Export Disabled Object Types** setting to exclude object types from an export when they are included in a Filtered List View.

This setting is related to the **Object Types to Exclude in Export** setting:

- **Export Disabled Object Types** excludes object types when they are in a view.
- **Object Types to Exclude in Export** excludes object types when they are not in a view. See [“Exclude object types from exports if they are not in a Filtered List View”](#) on page 629.

Applications > GRCM > Filtered List > Export Disabled Object Types

Default: blank

Values: In the **Value** field, type a comma-separated list of object type names that you want to exclude. For example, if you want to exclude Risk and Control object types, type: SOXRisk,SOXControl.

To exclude all object types, type \$ALL\$.

For example, suppose that you exclude SOXRisk and SOXControl. When users click **Export** in the PRSA Update filtered list view, the **Export** dialog box does not show check boxes for Risks, Controls, or descendants of controls. Although these object types are in the PRSA Update view, they are excluded from the **Export** dialog box.

Hide the Export feature in filtered list views for user profiles

Use the **Export Disabled Profiles** setting to hide the Export feature in filtered list views, based on the user's current profile.

This setting hides the **Export** button on the toolbar and the **Grid Actions > Export** menu option.

Applications > GRCM > Filtered List > Export Disabled Profiles

Default: blank

Values: In the **Value** field, type a comma-separated list of profile names that you want to prevent from exporting from views. For example, to hide the Export feature for users with the VRM Vendor and VRM Vendor Manager profiles, type: VRM Vendor,VRM Vendor Manager.

To hide the Export feature for all profiles, type \$ALL\$.

For example, suppose that you exclude VRM Vendor. When a user who is using the VRM Vendor profile opens a filtered list view, the **Export** button is not displayed on the toolbar and the **Grid Actions > Export** menu option is hidden.

Disable Bulk Update link in the Task Focused UI

In the Task Focused UI, this setting hides the **Bulk Update** link on the bulk update toolbar in Grid Views.

In the Standard UI, this setting has no effect.

If **Bulk Update Disabled in Task Focused UI** is set to false, other settings can be used to further refine the feature. For more information, see [“Exclude object types in Filtered List Views from bulk updates”](#) on page 631 and [“Hide the Bulk Update feature in filtered list views for user profiles”](#) on page 631.

Applications > GRCM > Filtered List > Bulk Update Disabled in Task Focused UI

Default: false

Values:

- true - the **Bulk Update** link on the bulk update toolbar in Grid Views is not displayed in the Task Focused UI
- false - the **Bulk Update** link on the bulk update toolbar in Grid Views is displayed in the Task Focused UI

Exclude object types in Filtered List Views from bulk updates

Use the **Bulk Update Disabled Object Types** setting to exclude object types from bulk updates. Use this setting to prevent users from updating information in multiple objects.

In an object type filtered list view in the Standard UI, this setting hides the **Bulk Update** link on the toolbar and the **Grid Actions > Bulk Update** menu option.

In views that contain multiple object types, this setting hides the excluded object types from the **Bulk Update** list. Descendents of the excluded object types are not hidden.

In the Task Focused UI, this setting hides the **Bulk Update** link on the bulk update toolbar in Grid Views by object type. Another setting controls overall functionality. For more information, see [“Disable Bulk Update link in the Task Focused UI” on page 630](#).

Applications > GRCM > Filtered List > Bulk Update Disabled Object Types

Default: blank

Values: In the **Value** field, type a comma-separated list of object type names that you want to exclude. For example, if you want to exclude Risk and Control object types, type: SOXRisk,SOXControl.

To exclude all object types, type \$ALL\$.

For example, suppose that you exclude SOXRisk. When users click **Bulk Update** in the PRSA Update filtered list view, the **Bulk Update** list does not show Risks. Although risk objects are in the PRSA Update view, users cannot edit them with the Bulk Update feature.

Hide the Bulk Update feature in filtered list views for user profiles

Use the **Bulk Update Disabled Profiles** setting to hide the Bulk Update feature in filtered list views, based on the user's current profile.

In the Standard UI, this setting hides the **Bulk Update** link on the toolbar and the **Grid Actions > Bulk Update** menu option.

In the Task Focused UI, this setting hides the **Bulk Update** link on the bulk update toolbar in Grid Views by profile. Another setting controls overall functionality. For more information, see [“Disable Bulk Update link in the Task Focused UI” on page 630](#).

Applications > GRCM > Filtered List > Bulk Update Disabled Profiles

Default: blank

Values: In the **Value** field, type a comma-separated list of profile names that you want to prevent from updating objects in bulk. For example, to hide the Bulk Update feature for users with the VRM Vendor and VRM Vendor Manager profiles, type: VRM Vendor,VRM Vendor Manager.

To hide the Bulk Update feature for all profiles, type \$ALL\$.

For example, suppose that you exclude VRM Vendor. When a user who is using the VRM Vendor profile opens a filtered list view, the **Bulk Update** link is not displayed on the toolbar and the **Grid Actions > Bulk Update** menu option is hidden.

Number of levels to export in the Filtered List View

Use the **Number of Levels to Export** setting to define how many total levels of object types the user can choose to export, including the top-level object that is exported.

This setting is useful for limiting the growth of the tree of objects that a user can export. The number of records that are exported grows exponentially as a user selects more object types to export. For example, if a user selects a single object type, such as Process, and chooses to export its Risks, the Controls under Risks, the Test Plans under Controls and the Test Results under Test Plans, it might result in hundreds or thousands of exported records. Unless the number of levels is limited, the export might take a long time, and might impact system performance for other users.

This setting is hidden by default. For information about unhiding settings, see [“Show hidden settings” on page 602](#).

The **Enable Object Type and Field Export Choices** setting overrides **Number of Levels to Export**. For more information, see [“Enable object type and field export choices in the Filtered List View” on page 629](#).

Applications > GRCM > Filtered List > Number of Levels to Export

Default: View+3

Values: Possible values are View, View+1, View+2, View+3, View+4, View+5, and so on.

In the Task Focused UI, the maximum value that is respected is View+5.

In the Standard UI, there is no maximum.

For example:

- If a user's **Grid View** is Process - Risk - Control, and this value is **View**, they can export Processes, their Risks, and their Controls. If this value is **View+1**, the user can export Processes, their Risks, and their Controls, and one more object type that is a direct child of Controls. If this value is **View+2**, the user can export one more object type that is a direct child of the first additional object type chosen. If this value is **View+3**, the user can export one more object type that is a direct child of the second additional object type chosen. The same pattern applies to **View+4** and **View+5**.
- If a user's **Filtered List View** is for Processes, and this value is **View**, they can export only Processes. If this value is **View+1**, the user can export Processes and one more object type that is a direct child of Process. If this value is **View+2**, the user can export one more object type that is a direct child of the first additional object type chosen. If this value is **View+3**, the user can export one more object type that is a direct child of the second additional object type chosen. The same pattern applies to **View+4** and **View+5**.

Note: This setting is case sensitive and there must be no spaces between the **View** value and the characters **+1**, **+2**, **+3**, **+4**, **+5**, and so on.

Maximum concurrent export requests in the Filtered List View

Use the **Concurrent Exports** setting to control the maximum number of Export to Excel (in .xls format) requests that are handled at the same time.

Applications > GRCM > Filtered List > Concurrent Exports

Default: 10

Values: In the **Value** field, type a number greater than zero.

Editable fields in a Filtered List View

Use the **Editable** setting to control whether users can edit the fields on a **Filtered List View** page.

A value of false makes all fields in the Filtered List View read-only. A value of true enables all fields in the Filtered List View to be edited. Actual ability to edit is controlled by security settings and field dependencies. Possible values are true or false.



Attention: If you change the registry settings to allow the Filtered List View to be editable, then *all* of the fields in the Filtered List View become editable. If there are any fields in the Filtered List View that you do not want to be editable, do *not* make the Filtered List View editable.

Applications > GRCM > Filtered List > Editable

Default: true

Values:

- true - all fields can be edited in a Filtered List View.
- false - no fields can be edited in a Filtered List View; the fields are read only.

Bulk move and rename setting

The Allow Hierarchical Moves setting determines whether users can perform hierarchical move operations. The setting also determines whether users can rename certain object types.

For move operations, the setting determines whether child objects are moved when their parent objects are moved with the  icon in Grid Views.

For rename operations, the setting determines whether a rename operation is allowed for the following object types: SOXBusinessEntity, SOXMilestone, self-contained object types, and object types that are used by the security model.

Applications > GRCM > Object Move > Allow Hierarchical Moves

Default: false

Values:

- true - no restrictions
- false

For move operations, child objects are not moved with parent objects for the following object types:

- SOXBusinessEntity
- SOXMilestone
- All objects types that are listed in the **Common > Security > Model** setting
- All object types that are listed in the **Common > Self Contained Object Types** setting

For rename operations, the following objects cannot be renamed:

- SOXBusinessEntity
- SOXMilestone
- Object types that are listed in the **Common > Security > Model** setting
- Object types that are listed in the **Common > Self Contained Object Types** setting

If a move or a rename involves a large number of objects, make the change after business hours to reduce the impact on system performance.

The Allow Hierarchical Moves setting applies only to the Task Focused UI.

Custom settings

When enabling new content types and creating your own reports, you may need to create your own custom registry settings. By default, you cannot create or delete settings until you enable the feature.

Common > Configuration > Allow Create and Delete Settings

Default: false

Values:

- **true** - enable the creation and deletion of custom settings.
- **false** - disable the creation and deletion of custom settings.

Creating a custom setting

After enabling **Allow Create and Delete Settings**, you can create custom settings entries in new or existing folders.

Complete the following procedure to create a custom setting:

Procedure

1. Log on to the Task Focused UI as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Navigate to the folder where the new setting will be located.
4. Click **Add Setting**.
5. On the Settings page, type a setting name, description, and value.
6. **Folder Path** contains the default folder where you started. Click **Choose** and select a different folder to change the folder.
7. Select **Encrypted** if you want the value of the setting to be encrypted.
8. Click **Add** to add the new setting to the selected folder.

Deleting a custom setting

After enabling **Allow Create and Delete Settings**, you can delete settings in new or existing folders.

Important: Do not delete any of the predefined settings shipped with IBM OpenPages. These settings are required and cause unexpected behavior in the application if they are removed.

Procedure

1. Log on to the Task Focused UI as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Navigate to the folder that contains the setting to be deleted. Select the desired setting. The **Delete** icon becomes active.

Note: If you select a folder, all settings within that folder are deleted.

4. Click **Delete**.

Copying settings and folders

You can copy individual settings to another location and copy folders to new folders. When you copy a folder, you can give the new folder a name. The settings and subfolders in the folder are copied to the new folder.

Procedure

1. Log on to the Task Focused UI as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Navigate to the folder where the source setting or folder is located.
4. Select the setting or folder that you want to copy.

5. Click **Copy To**.
6. If you are copying a setting, the **Copy Setting To** panel opens. Select the folder in which the new setting will be positioned.
7. If you are copying a folder, the **Copy Folder To** panel opens. Enter the name of the new folder in **Name** and choose a **Target Folder**.
8. Click **Done**. The new setting or folder is created.

Common folder settings

The registry settings in the Common folder are a select list of individual settings.

Maximum rows in exchange rate upload file

Define the **Maximum Import Rows** setting to limit the number of rows that can be in the CSV file that is used to upload currency exchange rates with the **Currencies** task in the Task Focused UI or the **Administration > Currencies** task in the Standard UI.

If a CSV file has more rows than defined in the setting, the upload fails and an error message is issued.

Maximum Import Rows

Common > Administration > Currencies > Upload > Maximum Import Rows

Default: 10,000

Values: In the **Value** field, type a number great than zero.

Use legacy associate

Controls whether associate operations use the new interface or the legacy interface.

You can use a registry setting to revert to using the legacy associate features in Activity Views and Detail Views only. This is to allow time to ensure that the new implementation meets your needs before you retire the old implementation.

Applications > Common > Configuration > Use Legacy Associate

The default value is **false**.

Permissible values are **true** or **false**.

Exclude characters from user names

When you create user names, you can exclude the use of any alphanumeric and special characters, including spaces, through the **Illegal Characters** setting.

For example, if you add an asterisk (*) as a value to this setting, the application validates the user name for that character before it was created. If it detects an asterisk (*) in the user name, such as Test*User, it displays an error message.

Common > Security > User Name > Illegal Characters

Default: none

Values: Type any characters (including spaces and punctuation marks) that you want to be considered as invalid when creating a user name. For example, if you want the asterisk (*) and ampersand (&) to be considered invalid in user names, enter *& in the **Value** field.

Set the system security model

By default, the security context point at which you can assign role templates to users on objects in the hierarchy is set at the Business Entity (SOXBusEntity) level. You can extend the security context to other objects in the hierarchy to achieve a finer level of control by changing the **Model** setting.

Important:

This is a system-wide setting. Switching the security model after data is loaded (or migrated) into the system is not recommended and requires assistance from IBM OpenPages with Watson Professional Services.

Common > Security > Model

Default:

Values: Type the object type names you want to use as security points.

The syntax for the **Model** setting is: SOXBusEntity/object_type-name

Example: To create a security point for assigning role templates at a Process level, you would enter:

```
SOXBusEntity/SOXProcess
```

Permissions in the Role template could then be assigned at either the Business Entity or Process level, and would include any objects that were created beneath that security context point in the same location.

The maximum number of security context points you can have in the **Model** setting is 3. For example, SOXBusEntity/SOXProcess/RiskAssessment

Disable access control on Role groups

When a role template is disabled, you can use the **Disable Role Group** setting to globally control the security access of users and groups who were previously assigned that role.

Common > Security > Role Templates > Disable Role Group

Default: false

Values:

- **true** - Users and groups who were previously assigned that role, will lose their access control and application permissions. A disabled role template is removed from the role assignment selection list and cannot be used for further role assignments.
- **false** - Users and groups who were previously assigned that role, will retain their access control and application permissions.

Related tasks

[“Enabling and disabling a role template” on page 115](#)

Configure self-contained object types

When you define an object type using the **Self Contained Object Types** setting, the behavior of that object type changes for copy, move, and rename operations.

A self-contained object type is an object type that has its own folder and is either part of the role-based security model as defined in the **Model** setting or defined using the **Self Contained Object Types** setting.

For information about the **Model** setting, see [“Role-based security model” on page 105](#).

Note:

- Roles can only be assigned to objects that are defined as security context points through the **Model** setting.
- Defining an object type through the **Self Contained Object Types** setting does not automatically change the folders of existing instances of that type. If instances of the object type you want to define as self-contained already exist, you must contact IBM OpenPages Support for assistance in executing a special PL/SQL script that will go back and create folders for existing instances. This script is maintained

by IBM OpenPages with Watson Customer Services & Support and does not ship as part of the product. Conversely, if an object type is later removed from the self-contained list, no automatic re-folding occurs. All existing instances retain their dedicated folders.

By default, Business Entities are self-contained objects. For example, if the role-based security model setting is defined as SOXBusEntity/SOXProcess, both Business Entity and Process objects are treated as self-contained objects.

Self-contained object types behave differently than non-self-contained object types for copy, move, and rename operations. The characteristics that distinguish self-contained objects from non-self-contained objects follow.

Self-contained objects:

- Are always created under a parent folder that matches the object name (the same behavior as Business Entities). For example, a process P1 under the North America business entity will have the path /North America/P1/P1.txt
- When copied, all the objects under its hierarchy will also be copied to the target.
- When moved, all the objects under its hierarchy will also be moved to the target.
- Can have only one parent of the same object type.
- Can only be moved to an allowed parent object.
- Cannot be moved to a folder.
- Cannot have their parent folder edited, moved, or renamed.
- Can be renamed by users who have Read+Write access control (ACLs) permission.
- During a copy operation, if a naming conflict exists between the source and the target object, the copy operation will fail and the naming conflict resolution choices made by a user are ignored.

Common > Self Contained Object Types

Default: none.

Values: In the **Value** field, type a comma-separated list of object type names.

For example, if you wanted Process and Risk Assessment object types, you would type: SOXProcess,RiskAssessment.

Applications > Common > Administration > System Files > Show GRC Folder Structure

Default: false

Values:

- true - _op_sox folder and subfolders are displayed
- false - _op_sox folder and subfolders are not displayed

Controls whether the GRC Object folder structure and system files are displayed in the  > **System Configuration > System Files** task.

Enable the CodeCogs Equation Editor in Rich Text fields

When you enable the CodeCogs Equation Editor with the **Enable CodeCogs(r) Equation Editors** setting, users can enter mathematical equations in Rich Text fields. The equations are rendered in all views. They are also represented in Cognos reports in HTML output.

In all Rich Text fields you can click the new **fx** icon in the toolbar to open a dialog where you can enter or update a mathematical equation. You can save and render an equation on the screen in both read only and edit mode. You can load or update them in a Rich Text field with ObjectManager and FastMap. You can also export them to Microsoft Excel from a Filtered List View or Grid.

The equation editor is only available in English.

There is source downloaded from a third-party web site, codecogs.com. If the equation editor is enabled, this site is automatically added to the security allow-list. The LaTeX version of a formula is sent to the CodeCogs web site, which returns an image of the formatted formula. If TLS/SSL is used, the formula is encrypted in transit. However, CodeCogs has access to your formula.

The formulas are displayed only in the Change History under the Source tab, not the Changes tab. In the Change History, an inserted or changed equation is highlighted in color in the Source tab. However, the color highlight is not currently supported for equations in the Changes tab.

Applications > Common > Rich Text Editor > Third Party plugins > Enable CodeCogs(r) Equation Editors

Default: false

Values:

- true - equation editor is enabled.
- false - equation editor is disabled.

Platform folder settings

The registry settings in the Platform folder are a select list of individual settings.

Enable custom REST service

Use the **Enable Custom REST Service** setting to extend the REST services with custom services that are not included in the existing API services.

For more information, see *Extend GRC API with Custom REST Services* in the *IBM OpenPages with Watson GRC REST API Guide*.

Platform > API > Enable Custom REST Service

Default: false

Values:

- true - to enable custom REST services
- false - to disable custom REST services

Compare Environments tool settings

You can configure the Compare Environments tool.

Settings for the Compare Environments tool are located in the **Platform > CompareEnvironments** folder.

Java heap size for the Compare Environments tool

Use the **Max Memory** setting to configure the maximum Java heap size, in megabytes, for the Compare Environments tool.

Platform > CompareEnvironments > Max Memory

Default: 4096

Values: In the **Value** field, type a number greater than zero.

Maximum number of rows to export from the Compare Environments tool

Use the **Export Max Rows** setting to control the maximum number of rows that can be exported to Microsoft Excel (in .xlsx format) from the Compare Environments tool.

If the number of rows to be exported exceeds the value of this setting, the results are truncated.

The maximum value of this setting is 1048576, which is the maximum number of rows that is supported by Microsoft Excel.

The default value of this setting is 100000. If you increase the value, you might need to increase the **Max Memory** setting to avoid errors.

Platform > Compare Environments > Export Max Rows

Default: 100000

Values: In the **Value** field, type a number greater than zero and less than or equal to 1048576.

Set localization options

You can configure settings in the Globalization folder to audit translation label changes and set a default language for IBM OpenPages with Watson.

Auditing

Platform > Globalization > Auditing Enabled

Default: true

Values: Enable auditing of changes that are made to translated object and application label text.

- **true** - auditing enabled.
- **false** - auditing disabled.

This option must be set to true to allow new application strings to load.

Default locale

Platform > Globalization > Default Locale

Default: en_US

Values: Set the language to use to display the application user interface by default.

Note: Users can override the default locale setting by choosing another language in the **My Settings** menu item option that is located under the user name.

The following list identifies the supported locale code values with their corresponding language:

- de_DE (German)
- en_GB (U.K. English)
- en_US (U.S. English)
- es_ES (Spanish)
- fr_FR (French)
- it_IT (Italian)
- ja_JP (Japanese)
- pt_BR (Brazilian Portuguese)
- zh_CN (Simplified Chinese)
- zh_TW (Traditional Chinese)

For example, to set the default language of the application interface to German, type de_DE in the **Value** field.

Configure primary associations

When a child object has multiple parent objects, the **Association Heuristic** setting controls how the system reassigns a new primary parent. The parent is assigned to a child object that is disassociated from its primary parent object. You can change how primary parent objects are reassigned to disassociated child objects.

Platform > Repository > Resource > Association Heuristic

Default: **Chronological**

Values: Type one of the following values:

- **Chronological** - the reassignment of a primary parent is based on the earliest creation date and time of an association.
- **Folder Context** - the reassignment of a primary parent is based on the folder path within the context of the business entity.

For example, control C1 has multiple risk parents: R1, R2, R3, and R4 (primary parent) and the object associations were created in the following chronological order:

Table 202. Parent folder path and associated child folder path	
Parent folder path	C1 Child folder path
/BE1/SBE2/R2	/BE1/SBE1/C1
/BE1/SBE1/R1	/BE1/SBE1/C1
/BE1/SBE3/R3	/BE1/SBE1/C1
/BE1/SBE4/R4 (primary parent)	/BE1/SBE1/C1

If you disassociate the primary parent, R4, from C1, although R2 is chronologically the earliest association to C1, R1 is reassigned as the primary parent. This is because R1 and C1's folder paths match (/BE1/SBE1).

Note: If no folder path matches the child object, the chronological order is used.

Configure the legacy move behavior

The Legacy Move Behavior setting controls how IBM OpenPages with Watson handles storage locations when a self-contained object is moved.

Platform > Repository > Resource > Move > Self-Contained Object Types > Legacy Move Behavior

Default: true

Values:

- **true** - objects that are stored within the self-contained object hierarchy are moved to a corresponding folder in the new location. Objects that are stored outside of the self-contained object hierarchy are left in their original location. Use this option if the location of the objects plays an important role in security or object management.
- **false** - the system uses hierarchical based logic when a self-contained objects is moved. All objects with primary associations are moved to the logical location dictated by the object relationship hierarchy. Use this option to allow the system to reorganize object storage so that it mirrors the relationship hierarchy.

Configure the host setting

If you have older JSP reports and want to send email notifications to users from these older JSP-based reports or the Notification Manager utility, configure the host setting.

Note: This setting is only used for backward compatibility.

Platform > Publishing > Mail

Default: none

Values: Click the name of a setting that is listed in the following table to open its detail page, and change the value as follows.

Table 203. Host settings	
Setting	Description
Enabled	Set the value to <code>true</code> .
From Address	Verify or enter the email address of the sender using a valid email address and format. By default, the value is: <code>sysadmin@yourcompany.com</code>
Host	Verify or enter the name of your mail server. By default, the value is: <code>mail.yourcompany.com</code>

Cross-context sharing

You can use the **Cross context sharing** setting to affect whether any non-primary links to objects outside the context (scope) of a copy operation are included or ignored during a copy operation.

When cross-context sharing is enabled, copy operations maintain non-primary links to objects outside the context of the copy. When it is disabled, non-primary links to objects outside the context of the copy are ignored.

For example, in the following example hierarchy, Control C1 was originally created under Risk R1, and R1 has a primary association to C1. Risks R2 and R3 have non-primary associations to C1. If a user copies Process P2 from BE2 to BE3, the link to C1 is maintained if the **Cross context sharing** setting is enabled (set to `true`). If the setting is disabled (set to `false`), the copied tree ends at R3 as the non-primary association to C1 is outside the context of the copy operation. If the user copies P1 from BE1 to BE3, the current state of the **Cross context sharing** setting is irrelevant. The non-primary association from R2 to C1 falls within the context of the copy operation.

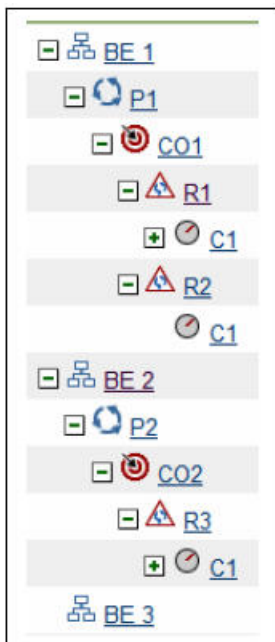


Figure 60. Sample Hierarchy

Platform > Repository > Resource > Copy > Cross context sharing

Default: false

Values: In the **Value** field, type one of the following values:

- **true** - Cross-context sharing is enabled and the copy operation maintains any non-primary links to objects that are outside the scope (context) of the copy.
- **false** - Cross-context sharing is disabled and the copy operation ignores any non-primary links to objects that are outside the scope (context) of the copy.

Platform Reporting Framework folder settings

The settings in the **Platform > Reporting Framework V6** folder apply to the reporting framework used by Cognos Analytics.

Note: In reference to Reporting Framework V6, V6 refers to the latest framework version, not to any specific OpenPages release number.

For more information, see the following topics:

- [Chapter 29, “Configuring and generating the reporting framework,” on page 951](#)
- [“Configuring settings that apply to all framework models” on page 957](#)
- [“Configuring framework models ” on page 961](#)

Reporting Schema folder settings

The **Platform > Reporting Schema** folder settings represent a selected list of individual settings.

Add indexes for fields in the reporting schema

You can add an index to any RT_ table in the database through the **Create Index on Fields** setting.

Before configuring this setting, complete the following tasks:

- Review this task with your database administrator and IBM OpenPages Support.
- Test the change by manually creating the index in the database before making a permanent change in IBM OpenPages with Watson.

You can create a string up to 4000 characters.

Configure this setting only after careful analysis of your data query patterns. Adding too many indexes to a table can harm performance.

Platform > Reporting Schema > Create Index on Fields

Default: none.

Values: In the **Value** field, enter an index in the following format:

```
ObjectTypeName1= [FieldGroupName1.PropertyName1,...,  
FieldGroupNameN.PropertyNameN]  
|ObjectTypeNameN= [FieldGroupName1.PropertyName1  
,...,FieldGroupNameN.PropertyNameN]
```

Where:

ObjectTypeName1 is the name of the object type you want to add an index to.

FieldGroupName1 is a bundle definition associated with the object.

PropertyName1 is the name of a property in the bundle.

Note:

- Vertical bars (|) separate multiple index strings.
- Commas (,) separates columns inside an index.

Depending on the size of the database, you can update the reporting schema through the application user interface or incrementally through scripts with assistance from IBM OpenPages Support.

For more information, see [“Changes that require the reporting schema to be updated or recreated” on page 159.](#)

Example 1: Adding an index on name and reporting period

You want to add an index on the Risk object type that includes the name and reporting period. The string would look as follows:

```
SOXRisk = [Core Attributes.Resource Name,  
Reporting Period Attributes.Reporting Period ID]
```

The Core Attributes bundle includes all of the following system parameters:

- Latest Resource Version
- Resource Check Out Status
- Resource Check-in Date
- Resource Checked in By
- Resource Checked Out By
- Resource Content Type
- Resource Creation Date
- Resource Creator
- Resource Description
- Resource File Type
- Resource Full Path
- Resource ID
- Resource Name
- Resource Parent Folder
- Resource Subresource Type
- Resource Type
- Resource Visibility

The Reporting Period Attributes bundle includes the following reporting period parameters:

- Reporting Period ID
- Reporting Period Name

Example 2: Adding an index on a custom field

You created a custom field called Test Reviewer on the Test object type and now want to add an index to this custom field. The index for the Test Reviewer custom field would be as follows:

```
SOXTest = [OpenPagesStandardTest.Test Reviewer]
```

Example 3: Adding an index for quick filters and custom simple strings

Indexes can help the performance of certain searches with Quick Filters and filters on custom simple string fields (except users and user groups).

The usual indexing technique is not applicable here, because Quick Filters and filters on custom simple string fields are commonly case insensitive and commonly implement "contains" logic. As such, even if a database index existed on the filtered field, it would not be used.

A typical use case is as follows:

- Filter performance appears inadequate.
- The user executing a filter has IBM OpenPages security access to a small fraction of the data.
- The number of records is high. This is a function of the number of object instances in the current reporting period and the number of reporting periods in the system.
- The width of records is high. This is a function of the number of custom properties.

For example, loss event data may be tightly restricted within a company. As such, indexing the LossEvent object type could improve filter performance.

```
LossEvent = [Reporting Period Attributes.Reporting Period ID,  
             Core Attributes.Resource Parent Folder]
```

It is beneficial to filter on security access before applying any property filter. The security access filter will filter out a large percentage of data, leaving the property filter to work on fewer records.

Such an index will benefit all the filters on a given Object Type, so it only needs to be created once per Object Type.

Security settings

The **Platform > Security** settings represent an individual settings to configure settings.

All of the following actions are accessed from the **Platform > Security** folder.

Redirect the security logoff link

By default, click **Log Off** in the header pane to log the user out of IBM OpenPages with Watson.

If you are using single sign-on (SSO), you can change the page that is displayed after you log off by modifying the value of **Logout URL**.

Note: If you are not using single sign-on, you cannot redirect the logout link.

Platform > Security > Logout URL

Default: none

Values: In the **Value** field, type a qualified URL.

Configure security for user login

Configure settings to prevent users from logging in to IBM OpenPages with Watson.

Locking a user account prevents the user from logging in to OpenPages with Watson. However, the user is still an active user in the system, and can be selected through the user selector.

Users can be locked automatically if they exceed a set number of unsuccessful login attempts. If the user is locked out because they forgot their password, you can unlock their account and reset their password from the **View, Edit, or Disable User** page. For more information, see [“Modifying user accounts” on page 86](#). If there is concern that the login attempts are malicious, contact your security department.

The **User Locking** folder contains the following settings that control the locking behavior of OpenPages with Watson.

Platform > Security > User Locking

Values: Click a setting to open its detail page, and type a value in the **Value** field.

Table 204. Locking values	
Value	Description
Enabled	Sets whether the User Locking settings are active. When the value is set to <code>true</code> , users are locked after they unsuccessfully try to log in more than the Maximum Allowed Attempts. If <code>false</code> , there is no limit to failed login attempts and the remaining settings are not honored.
Maximum Allowed Attempts	Sets the maximum number of times that a user can unsuccessfully try to log in to the application before the account is locked. The Unsuccessful Login Window setting applies a time window on the attempts.
Timeout	Sets the amount of time (in minutes) that the user account is locked after failing to log in. After the timeout is over, the user can attempt to log in again.
Unsuccessful Login Window	Sets a time window (in minutes) for the log in attempts. The system checks the number of failed attempts within the time window. For example, if the Maximum Allowed Attempts is '3', the Timeout is '60', and the Unsuccessful Login Window is '10': • If a user makes two unsuccessful login attempts and then waits 10 minutes, the account is not locked and the time window and number of attempts are reset to zero. The user can again make three attempts to log in. • If a user makes three unsuccessful login attempts within 10 minutes, the account is locked. The user must wait 60 minutes and can again make three attempts to login.

Security cross-site scripting filter settings

Cross-site scripting (XSS) is a computer security vulnerability that allows malicious attackers to inject client-side script into web pages viewed by other users. You can use the **Cross-site Scripting Filter** setting to check all HTTP GET requests sent to IBM OpenPages with Watson. The **Cross-site Scripting Filter** setting enables basic filtering of common attacks. The **Advanced XSS Filter** setting turns on more aggressive filtering of JavaScript actions. The **IE XSS Filter** setting is used to set the X-XSS-Protection header on a request. However, the preferred approach is to use the **X-XSS-Protection** header setting.

For more information about the **X-XSS-Protection** header setting, see [“Configure the HTTP response headers”](#) on page 647. If there is a conflict between the **IE XSS Filter** and **X-XSS-Protection** settings, the one that enables the header is used.

To allow certain HTML elements or attributes to pass through this filter, see [“Configure the security safe tags setting”](#) on page 646.



Attention: The XSS filter blocks attempts to save text fields that contain JavaScript. The XSS filter also blocks updates to items that were created and saved with JavaScript when the XSS filter was disabled. Text fields that contain JavaScript are not supported.

Note: These settings are hidden by default. To display them, see [“Show hidden settings”](#) on page 602.

Platform > Security > Cross-site Scripting Filter

Default: `true`

Values: In the **Value** field, type one of the following values:

- `true` - Cross-site filtering is enabled.
- `false` - Cross-site filtering is disabled.

Restart all application servers in your cluster to enable the change. For information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.

Platform > Security > Advanced XSS Filter

Default: `true`

Values: In the **Value** field, type one of the following values:

- `true` - Advanced XSS filtering is enabled.
- `false` - Advanced XSS filtering is disabled.

Restart all application servers in your cluster to enable the change. For information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.

Platform > Security > IE XSS Filter

Default: `false`

Values: In the **Value** field, type one of the following values:

- `true` - XSS filtering at the browser level is enabled.
- `false` - XSS filtering at the browser level is disabled.

Restart all application servers in your cluster to enable the change. For information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.

Configure the security safe tags setting

When the **Cross-site Scripting Filter** setting is enabled, certain HTML elements are blocked by that filter.

For more information on enabling this filter, see [“Security cross-site scripting filter settings”](#) on page 645. You can use the **Safe Tags** setting to globally allow certain HTML elements to pass through the filter.

For example, your company uses embedded forms to capture information that is provided by users. The embedded form contains the HTML `form` element, which is passed in an HTTP request. By default, the **Cross-site Scripting Filter** setting is enabled so the `form` element is blocked. To allow user input in an embedded form to be passed in an HTTP request, you would add the HTML `form` element to the **Safe Tags** value list as follows:

```
style, form
```

Tip: In the user interface, the **Safe Tags** setting is not displayed. You can add it manually in the XML file. Use the following path: `/OpenPages/Platform/Security/Safe Tags`

Safe Tags

Default: By default, the HTML `style` element is the only element that is allowed through the XSS filter.

Values: In the **Value** parameter, type the name of an HTML element or attribute. Multiple values must be separated by a comma.

Restart all application servers in your cluster to effect the change. For details, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.

Configure the HTTP response headers

Platform > Security > Headers

Configure the HTTP response header settings to add security that controls what a browser renders on a page. There are four settings:

- **Content-Security-Policy**

Controls from where the page can download source. If enabled, the value of this setting is merged with the value set by the system and added as a header to all page responses. The X-Content-Security-Policy header will also be set. The system value also includes the host name of the reporting server and some other settings required by the application.

The setting uses the Content Security Policy tool syntax. For more information, see [Content Security Policy](#).

Example value: `default-src myserver.com:100`

- **X-Frame-Options**

Controls where a page can get source to render in a frame. This header is added to all page responses. The value here overrides the default, which is SAMEORIGIN.

Example value: DENY

- **X-Content-Type-Options**

Prevents the browser from trying to determine the content-type of a resource that is different than the declared content-type. This header is added to all page responses. To override the default, enter an invalid string, for example, a space character.

Default: nosniff

- **X-XSS-Protection**

Enables X-XSS-Protection header on server responses. If X-XSS-Protection is set to true, the X-XSS-Protection header is set to `1; mode=block`. Using the X-XSS-Protection header setting is preferred to using the IE XSS Filter setting. If there is a conflict between the IE XSS Filter and X-XSS-Protection settings, the one that enables the header is used. For more information about the IE XSS Filter setting, see [“Security cross-site scripting filter settings”](#) on page 645.

Default: false

Configure allowed character combinations for URLs

You can use the **White-listed Suspicious Character Combinations** setting to enable certain character combinations in URLs.

By default, IBM OpenPages with Watson blocks URLs that contain unexpected or suspicious character combinations. If you attempt to go to a URL in OpenPages that contains unexpected characters, you are logged out of the application. See the `aurora.log` file on the application server for details about the character combination that was detected in the URL.

If OpenPages blocks URLs due to unexpected character combinations and the URLs are valid for your deployment, modify this setting to allow the character combination in URLs.

Note: Use a loader file to update this setting. Do not modify it in the user interface.

Platform > Security > White-listed Suspicious Character Combinations

Default: None

Values: Use a loader file to update the **Value** field.

Each character combination must be separated by a new line. Use `
` to create a new line.

If one of the characters that you want to allow is a special character, such as " (quotation mark), you must escape it, `"`;

For example, suppose you want to allow ' ; and " , . In this case, use a loader file like this sample file:

```
<openpagesConfiguration xmlFormatVersion="1.27">
<registry>
<registryEntry name="/OpenPages/Platform/Security/White-listed Suspicious Character
Combinations"
description="Certain character combinations are considered suspicious by the XSS filter. If
you see such a message in the aurora.log and the character combination is actually valid,
you can use this setting to allow it. Note that this setting may not be changed in the UI.
You must use a loader file."
hidden="false"
encrypted="false"
protected="true"
value="' ;&#xA;&quot;"/>
</registry>
</openpagesConfiguration>
```

Configure audit event settings

The audit event setting determines whether management events are audited.

Platform > Security > Audit Management Events

Default: false

Values: In the **Value** field, type one of the following values:

- **true** - Events related to users are audited. Examples of such events are: adding and modifying users and user groups, promoting and demoting a user to a superuser, enabling and disabling users, and adding and removing users from group memberships.
- **false** - Events related to users are not audited.

User Preferences folder settings

The User Preferences folder settings represent a selected list of individual settings in the User Preferences folder.

All of the following actions are accessed from the Platform folder.

Set alert notification behavior

Set which alert notifications are displayed to application users in the Alerts folder. You can select various alert notification settings in the **Alerts** page.

Application users can change these default settings through their **My Settings** pane.

User Preferences > Alerts

Default: false.

Values: Select the name of a setting on the **Alerts** pane to open its detail page. In the **Value** box, type one of the following values:

- **true** - An alert is displayed to application users.
- **false** - No alert is displayed to application users.

For example, you configured dependent fields or dependent picklists for an object type and you want to alert users that different values for particular fields are available depending on their selection. Under the Alerts folder, you can set the values in the **Picklist Options Changed** and **Picklist Values Removed** settings to **true** so each time a user changes a value in one of these fields, an alert notifying the user that values have changed is displayed.

Chapter 20. Configuring the global search feature

To optimize the performance of IBM OpenPages with Watson global search, you can enable or disable what can be searched, tune the search settings, and change other properties in the properties file.

About this task

For more information about using global search, see the topic *Searching for objects* in the *IBM OpenPages with Watson User Guide*.

Note: This feature is not applicable in IBM OpenPages for IBM Cloud Pak for Data.



Attention:

- Security rules and evaluating security rules adds a level of overhead to user operations, including global search. The more complex the rule, the more time it takes to evaluate the rule. The number of rules that are being implemented also affects performance.

In the case of global search, a security rule that extends read access can increase search time for users who do not have sufficient read access for an object type. Similarly, a security rule that restricts read access can increase search time for users who do have access to that object type through role-based security.

- Global search must be disabled before running the OPBackup and OPRestore utilities.

For information about configuring global search to use Secure Sockets Layer (SSL), see the following topics:

- [“Setting up a secure connection for the global search service” on page 806](#)
- [“Enabling a TLS database connection between the search server and the database server” on page 809](#)
- [“Disabling the TLS database connection between the search server and the database server” on page 810](#)

Setting up global search

Before you use IBM OpenPages with Watson global search in production (or even in a test environment against a large set of data), it is recommended that you first set up global search for a small set of data, such as a few thousand records in a test environment, and using the default settings.

Before you begin

Learn more about global search by reading the commonly asked questions listed in [“Global search FAQs” on page 675](#).

About this task

You can set up search on the same server as the one hosting the IBM OpenPages with Watson application. Make sure that the server has at least 12 GB of RAM to host both the IBM OpenPages with Watson application and search feature.

Procedure

1. Install IBM OpenPages with Watson using the default settings. Make sure that you also install the Search Server component. Specify the default values for all the fields. For more information, see the topic *Search server post installation tasks* in the *IBM OpenPages with Watson Installation and Deployment Guide*.

2. Follow the steps in the topic *Copying database driver files to the search server* in the *IBM OpenPages with Watson Installation and Deployment Guide* to copy the JDBC database driver and start the search server.
3. Log in to IBM OpenPages with Watson as a user with administrative privileges.
4. Switch to the Standard UI.

If you do not have the Standard UI, create the global search index by using the command line. For more information, see [How to automate solr tasks?](#).

5. Click **Administration** > **Global Search**
6. Click **Create** and periodically click **Refresh** to get progress updates.

The size of your data set, the configuration of your hardware, CPU speed, network speed, and available memory all influence the time it takes to set up global search. The process takes a few minutes on small sets of data (such as a few hundreds records) up to several hours on larger sets of data (such as a few million records).

What to do next

After global search is configured, it is ready to be accessed from both the Task Focused UI and the Standard UI.

Task Focused UI

You can configure UI components that provide users access to global search. For more information, see [“Adding a Search panel”](#) on page 370.

Standard UI

After search setup is completed, the search box is available beside the **Reporting Period** drop-down box. In the search box, type some text that you want to search on and press Enter. The result of your search appears in the result view. You can refine your search by typing more or fewer terms, or by selecting the object types to limit the search.

You can configure additional UI components that provide users access to global search. For more information, see [“Configuring users' Dashboard tabs”](#) on page 319.

For more information about using global search, see the topic *Searching for objects* in the *IBM OpenPages with Watson User Guide*.

For more information about administering global search, see [“Customizing global search”](#) on page 655

Setting login information for the search server

You can set the user names and passwords that the search server uses to access the database server and the IBM OpenPages with Watson global search service (Apache Solr). You can set the login information before you enable global search.

About this task

When you set up passwords, they are encrypted automatically to ensure secure and authenticated access.

If you have enabled global search and you want to change the login information, see [“Changing the database connection information for the search server”](#) on page 658.

Procedure

1. On the search server, open a command prompt.
2. To change the login information that the search server uses to login to the database, enter the following commands:

On Microsoft Windows operating systems,

```
cd <SEARCH_HOME>/OPSearch/opsearchtools/  
opsearchtool.cmd setdbuserpassword -username current-username -password "current-password"  
-newusername new-username -newpassword "new-password"
```

On Linux operating systems,

```
cd <SEARCH_HOME>/OPSearch/opsearchtools/  
./opsearchtool.sh setdbuserpassword -username current-username -password 'current-password'  
-newusername new-username -newpassword 'new-password'
```

Table 205. Parameters to change the database login information

Parameter	Description
<i>current-username</i>	The database username The value is the username that you entered in the OpenPages installation app when you configured the search server.
<i>current-password</i>	The password of the database user The value is the password that you entered in the OpenPages installation app when you configured the search server.
<i>new-username</i>	The new database username
<i>new-password</i>	The new password for the database user

For example, the following command changes the password to dbNEWpassword, but keeps the same database username:

```
opsearchtool.cmd setdbuserpassword -username dbuser -password "dbpassword"  
-newusername dbuser -newpassword "dbNEWpassword"
```

The following command changes both the database username and the password:

```
opsearchtool.cmd setdbuserpassword -username dbuser -password "dbpassword"  
-newusername dbNEWuser -newpassword "dbNEWpassword"
```

3. To change the login information for the global search service (Apache Solr), enter the following commands:

On Microsoft Windows operating systems,

```
cd <SEARCH_HOME>/OPSearch/opsearchtools/  
opsearchtool.cmd setsolruserpassword -newusername new-solr-username -newpassword new-solr-  
password
```

On Linux operating systems,

```
cd <SEARCH_HOME>/OPSearch/opsearchtools/  
./opsearchtool.sh setsolruserpassword -newusername new-solr-username -newpassword new-solr-  
password
```

Table 206. Parameters to change the global search service login information

Parameter	Description
<i>new-solr-username</i>	The new username for the Solr service The Solr user does not need to be an OpenPages user.
<i>new-solr-password</i>	The new password for the Solr user

Note: You do not need to provide the current username and password to change and encrypt the password for the global search service. The script uses the current login information of the database server for authentication before it allows the change. The default username and password is OpenPagesAdministrator / OpenPagesAdministrator.

For example, the following command sets the username to solruser and the password to solrpassword:

```
opsearchtool.cmd setsolruserpassword -username solruser -password solrpassword
```

4. Start the global search services.

For more information, see [“Starting the global search services by using a script” on page 844.](#)

5. If required, set up SSL for the Solr service.

For more information, see [“Setting up a secure connection for the global search service” on page 806](#)

What to do next

When you update the user name and password, the changes are applied only to the search server. You must update the database server as well to ensure the login information is synchronized.

Changing the login information for the search server

You can change the user names and passwords that the search server uses to access the database server and the global search service (Apache Solr).

About this task

When you change the passwords, they are encrypted automatically to ensure secure and authenticated access.

Procedure

1. Log on to OpenPages as a user with administrative privileges.
2. Switch to the Standard UI.
3. Click **Administration** > **Global Search**.
4. Click **Disable** to disable the global search component.
5. Stop the global search service.

For more information, see [“Stopping the global search services by using a script” on page 845](#) or [“Stopping the global search services” on page 847.](#)

6. Change the database user name or password.

For more information, see "Changing password references" in the *IBM OpenPages with Watson Administrator's Guide*.

7. Change the login information to use for the database server and Apache Solr.

For more information, see [“Setting login information for the search server” on page 650.](#)

8. Start the global search services.

For more information, see one of the following topics:

- [“Starting the global search services by using a script” on page 844](#)
- [“Starting the global search services on Windows” on page 845](#)
- [“Starting the global search services on Linux” on page 846](#)

9. In the Standard UI, click **Administration** > **Global Search**
10. Click **Enable** to enable the global search component.
11. If required, set up SSL for the global search service.

For more information, see [“Setting up a secure connection for the global search service” on page 806 in the IBM OpenPages with Watson Installation and Deployment Guide.](#)

What to do next

When you update the user name and password, the changes are applied only to the search server. You must update the database server as well to ensure the login information is synchronized.

Using OPBackup and OPRestore when global search is enabled

Before you run OPBackup or OPRestore, global search must be disabled.

About this task

OPBackup is the IBM OpenPages with Watson backup utility that backs up the necessary product files and database content on the server where it is run. The OPBackup utility creates a backup file that can be used by the OpenPages restore utility (OPRestore).

Procedure

1. Disable global search:
 - a) Log in as an administrator.
 - b) Click **Administration > Global Search > Disable**.
2. Perform OPBackup or OPRestore. For more information, see [“The OPBackup utility” on page 682](#).
3. Enable global search:
 - a) Log in as an administrator.
 - b) Click **Administration > Global Search > Enable**.



Attention: If you run the OPRestore utility, the search index becomes out of sync with the restored data in the OpenPages database. As a result, global search results might be inaccurate and incomplete. To prevent this, you must re-create the global search index. You can re-create the global search index before or after the database restore operation.

4. To re-create the global search index:
 - a) Log in as an administrator.
 - b) Click **Administration > Global Search > Disable**.
 - c) Click **Administration > Global Search > Drop**.
 - d) Click **Administration > Global Search > Create**.

Enabling and disabling global search

You can enable or disable global search.

About this task

For example, if your organization stipulates that you update passwords periodically, you can disable the global search component, reset user names and encrypt passwords, then enable the global search component.

Note: If the Global Search component is not enabled, then the Global Search Widget is not available for users to add to their **Dashboard** tabs. If you disable the Global Search component for a profile, then any existing Global Search widgets are removed from users' **Dashboard** tabs the next time they log on to OpenPages.

If you do not have the Standard UI, you can enable and disable global search by using the command line. For more information, see [How to automate solr tasks?](#).

Procedure

1. Log on to OpenPages with Watson as a user with administrative privileges.
2. Switch to the Standard UI.
3. Click **Administration > Global Search**.
4. Click **Disable** to disable the global search component.
5. Click **Enable** to enable the global search component again.

Enabling and disabling file attachment searching

From the global search administration page, you can toggle between enabling and disabling the file attachment search component for all search-enabled file types.

Before you begin

You must make sure that the openpages-storage location is accessible to the global search server before enabling file attachment search. For more information, see [“Setting the root path location for file attachment search” on page 674](#).

About this task

In a fresh installation, file attachment search is enabled by default. In an upgrade installation, file attachment global search is disabled.

Procedure

1. Log on to OpenPages with Watson as a user with administrative privileges.
2. Switch to the Standard UI.
3. Click **Administration > Global Search**.
4. Click **Disable File Search** to disable the file search component.
5. Click **Enable File Search** to enable the file search component again.
6. Click **Check for Updates**.
7. When the check for updates is completed, click **Update** for the changes to take effect.

Enabling attachment file types for global search

From the SOXDocument detail page, you can specify which MIME (Multipurpose Internet Mail Extensions) types are enabled or disabled for file attachment global search.

About this task

The column **Global Search** indicates for each file type whether it is enabled for global search.

Procedure

1. Log on to OpenPages with Watson as a user with administrative privileges.
2. Switch to the Standard UI.
3. Click **Administration > Object Types > SOXDocument**.
4. Under **File Types Information**, specify whether the file types selected by check box in the **Name** column are enabled or disabled for file attachment global search.
 - Click **Enable Search**. Selected file types that are disabled become enabled, and selected file types that are already enabled stay enabled.
 - Click **Disable Search**. Selected file types that are enabled become disabled, and selected file types that are already disabled stay disabled.

Note: Files might still be discovered after the file type of these files is disabled from search if the file type is associated with more than one MIME type. Files of this type are still discovered until all associated MIME types are excluded or are disabled from search. Follow the procedure [“Removing a file type from other object types”](#) on page 264 with each associated MIME type to remove the types from searches.

5. Click **Administration > Global Search**.
6. Click **Check for Updates**.
7. When the check for updates is completed, click **Update** for the changes to take effect.



Attention: Do not enable global search for file types that are binary, or that are media such as images, audio, and video. Global search ignores these file types, even if enabled.

The administrator must add or include a file type by using the **Add New** or **Include** pages before its global search setting can be changed.

Newly added or included file types are set to be disabled for file attachment global search by default.

Customizing global search

You can customize and configure global search to meet your organizational needs and policies.

Before you enable global search, you might want to evaluate your IBM OpenPages with Watson database schema and based on your organizational policy, determine which object types and their fields should be enabled for global search. As your IBM OpenPages with Watson database schema evolves, such as when you add or remove object types or fields, you can update global search to reflect those changes.

For information about configuring global search the first time you use it, see [“Example: customizing global search on initial enablement”](#) on page 656. For information about configuring global search after initial enablement, see [“Example: adding or removing object types and fields with an already-enabled global search”](#) on page 657.

Enabling or disabling object types or fields for global search

Most object types and fields that are already enabled for global search. You can change which object types and fields are enabled for global search before or global search is enabled.

About this task

For an example, see [“Example: customizing global search on initial enablement”](#) on page 656.

Changes to global search by enabling or clearing the **Global Search** check-box do not take effect until you use the **Check for Updates** command, followed by the **Update** command.

- After you add an object type or field to the reporting schema, you must decide whether the object type or field is enabled for global search or not. After you enable or clear **Global Search**, you must use the **Check for Updates** command, followed by the **Update** command.
- If you exclude a field from the reporting schema, disable global search for the field.
- After you enable or disable file attachment search, or after you add or remove MIME types from file attachment search, you must use the **Check for Updates** command, followed by the **Update** command. For more information, see [“Enabling and disabling file attachment searching”](#) on page 654 and [“Enabling attachment file types for global search”](#) on page 654.
- If you enable encryption on a field that is enabled for global search, you must disable global search before you can enable it for encryption. For more information, see [“Enabling and disabling global search”](#) on page 653. After you enable encryption, you must use the **Check for Updates** command, followed by the **Update** command.
- If you import object types and fields by using FastMap, and the imported data either has new object types or fields, or makes changes to existing object types or fields to the global search setting, you must use the **Check for Updates** command, followed by the **Update** command.

- If you import object types and fields by using Environment Manager or Object Manager, and the imported data has new object types or fields, or makes changes to existing object types or fields to the global search setting, you must use the **Check for Updates** command, followed by the **Update** command.
- If you delete an object type or a field, you must use the **Check for Updates** command, followed by the **Update** command.

Note: Anytime you click **Update**, some sort of reindexing takes place. However, when you click **Check for Updates**, no indexing occurs.

For example:

- When you add or remove fields from an object type, or add or remove MIME type from file search, this results in reindexing affected object types. The time this takes depends on how many records are under the affected object type.
- When you add a new object type, this results in reindexing the newly added object type. The time this takes depends on how many records are under the affected object type.
- Removing an object type does not result in reindexing that object type, other than the object type is removed from the index. This occurs immediately.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Switch to the Standard UI.
3. Click **Administration > Object Types**.
4. Select the object type or field for which you want to enable or disable global search.
5. Click **Edit**.
6. Enable or clear **Global Search**.
7. Click **Save**.
8. Click **Administration > Global Search**.
9. Click **Check for Updates**.
10. When the process completes, check the logs for changes such as added or removed object types and fields. You can go back and make more changes and click **Check for Updates** to see a log of updated changes.
11. When you are satisfied with your changes, click **Update** to force the changes onto the global search index.

Example: customizing global search on initial enablement

You can customize global search to meet your requirements when you first enable it.

About this task

This example assumes that you have not yet enabled global search. You decide to eliminate the object type **SOXSubaccount** and the field **Owner** of the object type **SOXRisk** from being searchable in global search.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. From the menu bar, click **Administration > Object Types**.
3. Select the object type **SOXSubaccount**.
4. Click **Edit** and clear **Global Search**.
5. Click **Save**.
6. From the menu bar, click **Administration > Object Types**.

7. Select the object type **SOXRisk**.
8. Under **Included Field Groups**, click **OPSS-Risk**.
9. Under **Field Definitions**, click **Owner**.
10. Click **Edit** and clear **Global Search**.
11. Click **Save**.
12. From the menu bar, click **Administration > Global Search** and click **Create**.
Create appears only on initial enablement.
13. Click **Refresh** periodically to get progress updates and notification of when the operation is complete.
This process can take from several minutes to several hours, based on how much data you have.

Example: adding or removing object types and fields with an already-enabled global search

After global search is enabled, you can add or remove object types and fields.

About this task

This example assumes that you have enabled global search based on the example in [“Example: customizing global search on initial enablement” on page 656](#). You now need to make changes such as adding to global search the object type **SOXSubaccount** and the field **Owner** of the object type **SOXRisk** so they are searchable. This example also assumes that you want to remove the field **Additional Description** from the field group of **MRG-BusEnt** of the object type **SOXBusEntity**.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. From the menu bar, click **Administration > Object Types**.
3. Select the object type **SOXSubaccount**.
4. Click **Edit** and enable **Global Search**.
5. Click **Save**.
6. From the menu bar, click **Administration > Object Types**.
7. Select the object type **SOXRisk**.
8. Under **Included Field Groups**, click **OPSS-Risk**.
9. Under **Field Definitions**, click **Owner**.
10. Click **Edit** and enable **Global Search**.
11. Click **Save**.
12. From the menu bar, click **Administration > Object Types**.
13. Select the object type **SOXBusEntity**.
14. Under **Included Field Groups**, click **MRG-BusEnt**.
15. Under **Field Definitions**, click **Additional Description**.
16. Click **Edit** and clear **Global Search**.
17. Click **Save**.
18. From the menu bar, click **Administration > Global Search** and click **Check for Updates**. You can look at the logs based on **Check for Updates** to find out what changes occurred.
19. Periodically, click **Refresh** to get progress updates and notification of when the operation is complete.
This process can take from several minutes to several hours, based on how much data you have.
20. Click **Update** to start an update operation so that your global search index is synced with the changes you made.
21. Click **Refresh** periodically to see how far from completion the process is. This process can take from several minutes to several hours, based on how much data you have and the kind of changes you made.

Global search is now updated and ready for use.

During the **Update** operation, global search is offline. Any user who attempts to use global search receives a message to this effect. Plan an update during off-hours, and communicate the scheduling of the update to your users.

Changing the database connection information for the search server

You can change the connection information that the search server uses to access the database server.

Procedure

1. Disable global search and stop the global search services.

For more information, see [“Stopping the global search services by using a script” on page 845](#) or [“Stopping the global search services” on page 847](#).

2. Log on to the search server as a user with administrative privileges.
3. Go to <SEARCH_HOME>/OPSearch/opsearchtools/.
4. Open the `openpages_search.properties` file in a text editor.
5. Modify the database connection properties to meet the needs of your environment.

Use the following examples as a guide.

IBM Db2

```
# Database connectivity information
OPSearchTool.DatabaseType = DB2
OPSearchTool.DbaseHostName = OP73-WIN-DB2
OPSearchTool.DatabasePort = 50000
OPSearchTool.DatabaseName = OPX
OPSearchTool.DatabaseUserID = openpages_db_user_id
OPSearchTool.DatabasePassword = openpages_db_password
```

Oracle

```
# Database connectivity information
OPSearchTool.DatabaseType = Oracle
OPSearchTool.DbaseHostName = OP73-WIN-ORACLE
OPSearchTool.DatabasePort = 1521
OPSearchTool.DatabaseName = OPX
OPSearchTool.DatabaseUserID = openpages_db_user_id
OPSearchTool.DatabasePassword = openpages_db_password
```

6. Encrypt the database password in the search properties file.

The database password that you entered in the `openpages_search.properties` file is in plain text. Change the password to encrypt it. For more information, see [“Setting login information for the search server” on page 650](#).

7. Start the global search services.

For more information, see one of the following topics:

- [“Starting the global search services by using a script” on page 844](#)
- [“Starting the global search services on Windows” on page 845](#)
- [“Starting the global search services on Linux” on page 846](#)

Displaying a custom field in global search results

The administrator can configure one additional custom field to be displayed in the search results for each object type.

About this task

By default, search results return the Name, Description, and Folder Path field values. For some object types, those fields might not contain enough details about the record to help users determine whether the record they are looking for is in the search result. As administrator, you can customize global search results to contain one additional field in the search results to help users.

This additional field is configured globally across profiles.

The additional field supports text area and text box display types only. If any other display type is used, the search results might not display the field value correctly.

Procedure

1. Log on to OpenPages with Watson as a user with administrative privileges.

2. Click  > **System Configuration** > **Settings**.

Or, in the Standard UI, click **Administration** > **Settings**.

3. Click **Platform** > **Search** > **Result Fields**

4. Locate the object type for which you want to add an additional field to the search result.

If the object type for which you want to add the additional field is not listed, select **Result Fields** by clicking the check box next to it, and then click **Add Setting** to create it.

5. Select the setting for which you want to add additional field for that object type.

6. Set or change the value by using the following format: *Field-Group.Field-Name*.

The additional field value appears after the Description system field on a new line in the items returned from a global search. For example, OPSS-LossEv.What Happened displays the text of the field What Happened in the search result. If the field does not have any value, the field name is shown in the result, but with no value.



Attention: You must provide the correct field group and field name for the additional field. If the formatting is wrong, or if the field group or field name do not match what is in your OpenPages schema, that additional field is not included in the search results.

You can ensure that you use the correct field group and field name by going to the source. For example, to add a field to the Workpaper object type search results:

Note: This example uses the Standard UI. The process is similar in the Task Focused UI.

- a. Log on to OpenPages with Watson as a user with administrative privileges.
- b. Select your object type. Click **Administration** > **Object Types** > **Workpaper**.
- c. Select your field-group. From **Included Field Groups**, click the field group **OPSS-Work**.
- d. Select your field-name. From **Field Group Information**, find the name of the custom field you want to add. For example, **Audit Description**.
- e. Make sure that you have the field group and field name correct, for example, OPSS-Work.Audit Description. Follow the steps in the preceding procedure. For example, click **Administration** > **Settings** > **Platform** > **Search** > **Result Fields** > **Workpaper**.
- f. Set or change the value to OPSS-Work.Audit Description and click **Save**. The additional field value Audit Description appears after the Description system field on a new line in the items that are returned from a global search.

Global search settings

You can tune and customize global search to suit your organizational needs and policies.

Some settings are already optimized and do not need any changes. Some are preset on initial installation of IBM OpenPages with Watson. And some require attention if you make changes to global search. This section lists the available settings for global search, with a summary of what they do, and explains when you might need to make changes to settings.

There are also search properties that are not specified in settings. For more information, see [“The global search properties file”](#) on page 671.



Attention: Where you are told "Do not need to modify this setting unless you are instructed to do so by customer support", do not modify the setting without consulting first with IBM OpenPages Support. Changing these settings can result in global search not working or unexpected performance issues.

Many global search settings are set as hidden by default. You must unhide them first. For more information, see [“Unhiding the hidden global search settings”](#) on page 660.

Unhiding the hidden global search settings

Many global search settings are set as hidden by default. Before you can change the global search settings, you must unhide them.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Applications** > **Common** > **Configuration** and select **Show Hidden Settings**.
4. Change the value from **false** to **true**.

You can now see all of the settings in your IBM OpenPages with Watson environment.

Setting the Query Path to the global search administration server

Specifies the query path to the search server that handles administration.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Admin** > **Query Path**.
4. Change the value as required.



Attention: Do not modify this setting unless you are instructed by IBM OpenPages Support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the URL to the global search administration server

Specifies the URL path to the IBM OpenPages global search server that handles administration.

About this task

The value of this setting is set based on your initial installation of global search. If you decide to reinstall global search on a different server, or enable SSL, or select a different port value, you must make the appropriate change. If you enable SSL, then change http to https. If you change the server on which global search is installed, you must provide the server host name or the IP address. If you need to use a different port other than the default, you must specify the different port.



Attention: Before you change this setting, make sure that global search is disabled. For more information, see [“Enabling and disabling global search”](#) on page 653.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Admin** > **Search Server Administration URL**.
4. Change the value as required.



Attention: If you are changing this setting because you want to enable SSL or because you want to change the server on which global search is installed, then you must also make the same change to the settings **Platform** > **Search** > **Index** > **Search Server URL** and **Platform** > **Search** > **Request** > **Search Server URL**.

Setting the progress refresh interval

Specifies the frequency (in seconds) of updating progress in the IBM OpenPages with Watson.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Full** > **Progress Refresh Interval**.
4. Change the value as required. The default value is 30 seconds.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the number of records to cache

Specifies the total number of records to cache before sending to the Apache Solr server for indexing.

About this task

If you increase the value of this setting, the initial full index might take less time, depending on your system configuration and database provider. However, this might require more RAM, CPU, and network resources. See the section on global search properties on how to increase the available memory to offset out-of-memory issues if you make a change to this setting.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.

3. Click **Platform > Search > Index > Full > Record Cache Size**.
4. Change the value as required. The default value is 100.



Attention: Do not modify this setting unless you are instructed by IBM OpenPages Support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the polling interval

Specifies the polling interval (in seconds) to check for changes (added, modified, or deleted) in IBM OpenPages with Watson objects.

About this task

By default, global search checks every minute if your data changes in the IBM OpenPages with Watson database. If the database contains changes, global search syncs up the search index so that when users search, those changes are reflected in the search result.

Reducing the polling interval means that the search index is more in sync with the database changes. However, this might result in slower database performance that impacts other IBM OpenPages with Watson operations, as well as slower search performance due to more frequent updates. Based on the load of your system and available resources, you might find you must increase this value to 300 (5 minutes) to offset the load. If you change this value, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search” on page 653](#).

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration > Settings**.
Or, in the Standard UI, click **Administration > Settings**.
3. Click **Platform > Search > Index > Incremental > Polling Interval**.
4. Change the value as required. The default value is 60.

Setting the number of records to cache before sending to the server for indexing

Specifies the total number of records to cache before sending to the Apache Solr server for indexing.

About this task

If you increase the value of this setting, the initial full index might take less time, depending on your system configuration and database provider. However, this might require more RAM, CPU, and network resources. See the section on global search properties on how to increase the available memory to offset out-of-memory issues if you change this setting.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration > Settings**.
Or, in the Standard UI, click **Administration > Settings**.
3. Click **Platform > Search > Index > Incremental > Record Cache Size**.
4. Change the value as required. The default value is 100.



Attention: Do not modify this setting unless you are instructed by IBM OpenPages Support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the Query Path to the Apache Solr server that handles Folder ACL indexing

Specifies the URL path to the Apache Solr server that handles Folder ACL indexing.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Folder ACL Query Path**.
4. Change the value as required.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the language analyzer that is used by search

Specifies the two or three letter abbreviation for the language analyzer that is used by search, that is, the language that search is optimized for.

Before you begin

If global search is already enabled, disable global search and drop the current index. For more information, see [“Enabling and disabling global search” on page 653](#).

About this task

Search results might be of different quality for other languages. For best results, use one of the supported locale languages: en=English (US or UK), pt=Brazilian Portuguese, fr=French, de=German, it=Italian, ja=Japanese, es=Spanish, cjk=Chinese, Japanese, Korean, zh=Simplified Chinese.

The value of this setting is set based on your initial installation of global search. If after installing global search you decide to change the language locale of your database data, you must modify the value of this setting to reflect the language of your text. If your data has mixed language text, such as English and Chinese, pick the language in which most of your data is created; this language becomes the main language for which global search is optimized.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Language Analyzer**.
4. Change the value as required. The default value is **en**.



Attention: Before you make a change to this setting, if global search is already enabled, make sure to disable global search and drop the current index. For more information, see [“Enabling and disabling global search” on page 653](#).

Setting the Query Path to the Apache Solr server that handles Folder ACL indexing

Specifies the URL path to the Apache Solr server that handles indexing.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Query Path**.
4. Change the value as required.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the URL to the Apache Solr server that handles Folder ACL indexing

Specifies the URL for the search server index.

About this task

The value of this setting is set based on your initial installation of global search. If you decide to reinstall global search on a different server, or enable SSL, or select a different port value, you must make the appropriate change. If you enable SSL, then change http to https. If you change the server on which global search is installed, you must provide the server host name or the IP address. If you need to use a different port other than the default, you must specify the different port



Attention: Before you make a change to this setting, make sure that global search is disabled. For more information, see [“Enabling and disabling global search” on page 653](#).

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Search Server URL**.
4. Change the value as required.



Attention: If you are changing this setting because you want to enable SSL or because you want to change the server on which global search is installed, then you must also make the same change to the settings **Platform** > **Search** > **Admin** > **Search Server Administration URL** and **Platform** > **Search** > **Request** > **Search Server URL**.

Setting the number of records inserted per batch

Specifies the number of search results records that are inserted per batch.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Batch Size**.
4. Change the value as required. The default value is 1000.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the Query Path to the Apache Solr server that handles Folder ACL search requests

Specifies the URL path to the Apache Solr server that handles Folder ACL search requests.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Folder ACL Query Filter**.
4. Change the value as required.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the URL to the Apache Solr server that handles OpenPages search requests

Specifies the URL path to the Apache Solr server that handles search requests.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Query Path**.
4. Change the value as required.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the number of attempts to fill the search results

Specifies the number of attempts to fill the search results defined in **Search Page Size** with viewable records after security is applied on **Result Cache Size** items.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Result Cache Refill Attempts**.
4. Change the value as required. The default value is 5.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the number of search results records that are cached per user session

Specifies the number of search results records that are cached per user session. This value sets the upper limit for the number of results that are shown to the user.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Result Cache Size**.
4. Change the value as required. The default value is 100.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the internal page size for search results

Specifies a two-number value that controls the total number of results that Apache Solr returns.

About this task

Results that come back from Solr are post processes, and only those results that meet the security rules of the user are kept and presented to the user. If a user has a restrictive security rule and policy, it is possible that most of what is in the initial page of 500 items might be eliminated in an attempt fill the cache setting that is specified in **Platform** > **Search** > **Request** > **Result Cache Size**. If so, an additional 10,000 items are retired from Apache Solr and are post processed.

If your organization uses a complex security model, and many of your users have restrictive security rules and policies, chances are they see fewer results than expected. Advise those users to refine their search terms. You can also help users by increasing the value of this setting. Increasing the value of this setting might impact search performance.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Search Page Size**.
4. Change the value as required. The default value is 500|10000.



Attention: Do not modify this setting unless you are instructed by IBM OpenPages Support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the URL to the Apache Solr server that handles search requests

Specifies the URL for search requests.

About this task

The value of this setting is set based on your initial installation of global search. If you decide to reinstall global search on a different server, or enable SSL, or select a different port value, you must make the appropriate change. If you enable SSL, then change http to https. If you change the server on which

global search is installed, you must provide the server host name or the IP address. If you need to use a different port other than the default, you must specify the different port



Attention: Before you change this setting, make sure that global search is disabled. For more information, see [“Enabling and disabling global search”](#) on page 653.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Search Server URL**.
4. Change the value as required.



Attention: If you are changing this setting because you want to enable SSL or because you want to change the server on which global search is installed, then you must also make the same change to the settings **Platform** > **Search** > **Admin** > **Search Server Administration URL** and **Platform** > **Search** > **Index** > **Search Server URL**.

Setting a time limit to search before timing out

Specifies the approximate time (in milliseconds) for Apache Solr to search before timing out.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Search Timeout**.
4. Change the value as required. The default value is 0.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting an additional field in the search result set

s Specifies an additional field for an object type to be returned as part of the search result set.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Result Fields** > *<object type name>*.
4. For details on how to change or provide a new value, see [“Displaying a custom field in global search results”](#) on page 659.
5. If the object type for which you want to add the additional field is not on the list, you can create a new setting for it. Select the **Result Fields** node and click **Add Setting**.

Setting whether to allow compression

Specifies whether the data being passed between the Apache Solr server and IBM OpenPages with Watson is compressed.

Procedure

1. Log in to OpenPages with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Allow Compression**.
4. Change the value as required. The default value is **true**.



Attention: Do not modify this setting unless you are instructed to do so by customer support. Changing this setting can result in global search not working or unexpected performance issues.

Setting the network connection request timeout

Specifies the network connection request timeout (in milliseconds) to the Apache Solr server.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Connection Timeout**.
4. Change the value as required. The default value is 5000.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting whether to allow URL redirects

Specifies whether URL redirects are allowed.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Follow Redirects**.
4. Change the value as required. The default value is **false**.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the number of allowed connections from the platform

Specifies the number of allowed connections to the Apache Solr server from IBM OpenPages with Watson.

Procedure

1. Log in to OpenPages with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.

3. Click **Platform > Search > Maximum Connections Per Host**.
4. Change the value as required. The default value is 100.



Attention: Do not modify this setting unless you are instructed to do so by customer support. Changing this setting can result in global search not working or unexpected performance issues.

Setting the number of allowed connections

Specifies the total number of allowed connections to the Apache Solr server.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration > Settings**.
Or, in the Standard UI, click **Administration > Settings**.
3. Click **Platform > Search > Maximum Total Connections**.
4. Change the value as required. The default value is 1000.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the number of times a request is reattempted

On error, specifies the number of times a request is reattempted before reporting a request failure.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration > Settings**.
Or, in the Standard UI, click **Administration > Settings**.
3. Click **Platform > Search > Request Retry Attempts**.
4. Change the value as required. The default value is 3.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the socket timeout for indexing

Specifies the socket connection timeout (in milliseconds) to the Apache Solr server for indexer use.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration > Settings**.
Or, in the Standard UI, click **Administration > Settings**.
3. Click **Platform > Search > Socket Timeout (index)**.
4. Change the value as required. The default value is 1800000.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the socket timeout for searching

Specifies the socket connection timeout (in milliseconds) to the Apache Solr server for search use.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Socket Timeout (search)**.
4. Change the value as required. The default value is 5000.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the Apache Solr password

Specifies the Apache Solr password to authenticate against the user ID.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Solr Password**.
4. Change the value as required. The default value is encrypted text.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the Apache Solr user ID

Specifies the Apache Solr user ID to authenticate against the server.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Platform** > **Search** > **Solr User ID**.
4. Change the value as required. The default value is 0.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the default number of search results to return per page

Specifies the default number of search results to return per page.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.

2. Click  > **System Configuration** > **Settings**.
Or, in the Standard UI, click **Administration** > **Settings**.
3. Click **Applications** > **GRCM** > **Search** > **Default Results Page Size**.
4. Change the value as required. Allowable values are **10**, **25**, and **50**. The default value is **10**.



Attention: If you change the value of this setting to a value larger than 10, global search and the overall performance OpenPages might be impacted. This change is global to all users.

The global search properties file

To customize global search, you can specify properties in the global search properties file.

The property file is named `openpages_search.properties`, and is located in `<SEARCH_HOME>/OPSearch/opsearchtools/`. If you make changes to this file, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search” on page 653](#).

Some changes might require you to drop the global search index and re-create it.

Most properties in this file are set to the default value. Only those properties that you might need to interact with are documented; the rest must not be modified unless you are instructed to do so by IBM OpenPages Support.

You can also use settings to tune and customize global search. For information about specifying the settings, see [“Global search settings” on page 660](#).

Setting the error handling parameters for the indexer

Use this property to set error handling parameters for the indexer that it might run into.

About this task

During indexing (both full and incremental) the indexer can run into issues such as bad records, database errors, network issues, and so on. If so, the indexer attempts to recover from those issues and continue indexing instead of ending. It does so by entering an error-handler mode, indexing until it recovers from the error or reaches a number of retries. Those parameters are set by using four values of **Major**, **Minor**, **Panic**, and **PanicLimit**.

By default, indexing is performed on an object type by processing all records in that object type in one continuous process. If an error is encountered, the indexer enters an error-handler mode. In this mode, it processes a chunk of 100 records (the value for **Major**) at a time. If it still runs into an issue, it scales back to a chunk of 10 records (the value for **Minor**) and if it still runs into an issue, it scales back to a chunk of one record (the value for **Panic**). If it still runs into issues, it attempts up to **PanicLimit** times before giving up and skipping that record from the index, and it goes back to the chunk of **Major** after which it goes back to normal indexing without chunking.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the `<SEARCH_HOME>/OPSearch/opsearchtools/` folder.
3. Open the `openpages_search.properties` file.
4. Change the **OPSearchTool1.IndexerErrorHandlerParameters** property as required.



Attention: If you change to the `openpages_search.properties` file, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search” on page 653](#).

Setting the maximum opsearchtool.jar heap size

Use this property to set the maximum heap size, in megabytes, to be used by `opsearchtool.jar` for general operations.

About this task

You might need to increase the value of the **OPSearchTool.SearchToolHeapSize** property if you encounter out-of-memory issues during general `opsearchtool.jar` operations. The out-of-memory issues might be due to the complexity of an OpenPages schema that contains many profiles, object types, field groups, and fields.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the `<SEARCH_HOME>/OPSearch/opsearchtools/` folder.
3. Open the `openpages_search.properties` file.
4. Change the **OPSearchTool.SearchToolHeapSize** property as required.



Attention: If you change to the `openpages_search.properties` file, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search”](#) on page 653.

Setting the maximum Apache Solr heap size

Use this property to set the maximum heap size, in megabytes, to be used by Apache Solr.

About this task

You might need to increase the value of the **OPSearchTool.SolrHeapSize** property if you encounter out-of-memory issues while indexing or searching. The out-of-memory issues might be due to the size of your records or the number of records that are indexed.

If you increase the heap size and you do not have sufficient free memory on the system, you might cause further out-of-memory issues and experience performance issues with global search.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the `<SEARCH_HOME>/OPSearch/opsearchtools/` folder.
3. Open the `openpages_search.properties` file.
4. Change the **OPSearchTool.SolrHeapSize** property as required.



Attention: If you change to the `openpages_search.properties` file, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search”](#) on page 653.

Setting the maximum opsearchtool.jar heap size during indexing

Use this property to set the maximum heap size, in megabytes, to be used by the `opsearchtool.jar` file during indexing.

About this task

You might need to increase the value of the **OPSearchTool.IndexerHeapSize** property if you run into out-of-memory issues during full indexing or incremental indexing.

The out-of-memory issues might be due to the size of your records that are indexed.

If you increase the heap size and you do not have sufficient free memory on the system, you might cause further out-of-memory issues and experience performance issues with global search.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ folder.
3. Open the openpages_search.properties file.
4. Change the **OPSearchTool1.IndexerHeapSize** property as required.



Attention: If you change to the openpages_search.properties file, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search”](#) on page 653.

Setting the maximum text extraction heap size for indexing

The **OPSearchTool1.TextExtractorHeapSize** is used to handle the indexing of file attachments when the amount of extracted text is large. The property sets the maximum heap size, in megabytes, to use. Once the total is reached, the files are immediately added to Solr before adding any others. This property helps to minimize possible memory related issues.

About this task

If you encounter out-of-memory issues during full indexing or incremental indexing, increase the value of the **OPSearchTool1.TextExtractorHeapSize** property. The out-of-memory issues might be due to the size and complexity of your file attachments.

If you do not have sufficient free memory on the system for the heap size that you configured, you might cause further out-of-memory issues and experience performance issues with global search.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ folder.
3. Open the openpages_search.properties file.
4. Change the **OPSearchTool1.TextExtractorHeapSize** property as required.



Attention: If you change to the openpages_search.properties file, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search”](#) on page 653.

Setting the text extractor timeout limit

Use this property to limit how long, in milliseconds, to wait for the text extractor to extract text from file attachments during indexing.

About this task

You might need to increase the value of the **OPSearchTool1.TextExtractorTimeout** property during full indexing or incremental indexing.

The timeout issues might be due to the size and complexity of your file attachments or the limits of your overall system performance.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ folder.

3. Open the `openpages_search.properties` file.
4. Change the **OPSearchTool.TextExtractorTimeout** property as required.



Attention: If you change to the `openpages_search.properties` file, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search”](#) on page 653.

Setting the maximum text to extract from file attachments for indexing

Use this property to set the maximum text string, in megabytes, to extract from file attachments for indexing.

About this task

The **OPSearchTool.FileExtractionSize** property helps to prevent out-of-memory errors during the indexing of large file attachments.

By default, the maximum text string that is extracted from file attachments for indexing is 500 MB.

If you increase the value of the **OPSearchTool.FileExtractionSize** property, the indexing process might run more quickly but you might encounter out-of-memory issues during full indexing or incremental indexing.

If you decrease the value, the indexing process runs more slowly but you might avoid the out-of-memory issues.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the `<SEARCH_HOME>/OPSearch/opsearchtools/` folder.
3. Open the `openpages_search.properties` file.
4. Change the **OPSearchTool.FileExtractionSize** property as required.



Attention: If you change to the `openpages_search.properties` file, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search”](#) on page 653.

Setting the root path location for file attachment search

Use this property to set the file storage root path location for file attachment search.

About this task

When OpenPages search server is on a different server than the OpenPages application server, the search server must have access to the OpenPages file storage location in order for it to index file attachments. If the search server is on a Windows operating system, you can use either the Uniform Naming Convention (UNC) or Local File System (LFS) path. If the search server is on a Linux operating system, you must use the LFS path.

Windows UNC path example:

```
\\\\\\OPAppServer\\shared\\OpenPages\\openpages-storage
```

Windows FLS path example:

```
C:\\shared\\OpenPages\\openpages-storage
```

Linux FLS path example:

```
/shared/OpenPages/openpages-storage
```



Attention: You must double the “\” character in the UNC and FLS path on Windows, otherwise the path is not properly processed.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ folder.
3. Open the openpages_search.properties file.
4. Change the **OPSearchTool1.FileStorageRootPath** property as required.

Global search FAQs

Questions are sometimes asked about global search and how it works.

Global search indexing

Q. How does the indexing work?

A. IBM OpenPages global search server includes an indexing service. When you click **Create** in the Administration UI, the indexing service queries the OpenPages database for records of object types and fields that are enabled for global search. Those records are read, formatted, and then indexed by Apache Solr. The index is later used for search when the global search feature is used from the OpenPages UI.

This one-time initial indexing is called full indexing. After full indexing is complete, the global search indexer service enters an incremental indexing mode. Incremental indexing mode queries the OpenPages database once a minute for modified records, newly added records, or deleted records of object types that are enabled for global search and reindexes them to keep the global search index in sync with the OpenPages data.

Q. Does global search crawl the network-attached storage (NAS) (openpages-storage location)?

A. OpenPages uses file storage, and shares the file storage location across all instances of OpenPages applications. By default, OpenPages global search is configured with file search enabled. So yes, if file search is enabled, access to openpages-storage location must be set for global search. For more information, see [“Setting the root path location for file attachment search” on page 674](#).

Q. Are there any regularly scheduled batch jobs?

A. Yes, there is a regularly scheduled batch job that runs. The indexer (when it is running in incremental indexing mode) runs as a regularly scheduled batch job.

Q. Are the indexes and logs stored on a local drive?

A. OpenPages global search index is a proprietary format of Apache Solr, and is stored on the local hard disk drive where the global search server is installed. OpenPages global search can be installed on any local hard disk drive on the system where you installed global search. For optimal performance, it is best to install global search on a separate solid-state drive, that is, not on the same drive as the operating system.

Q. How is the index used by the product?

A. The index is proprietary to Apache Solr, is used by Apache Solr only, and is stored on the local file system where global search is installed. The index is accessed and updated anytime global search is indexing in both full and incremental mode, and the index is looked up anytime an OpenPages user is running a search using global search.

Q: If I don't have the Standard UI, how do I drop and re-create the index?

The user interface for administering global search is not available in the Task Focused UI. Instead, you can administer global search by using the command line. For more information, see [How to automate solr tasks?](#).

Sizing and scaling

Q. The documentation mentions that global search can be run only as a single instance.

A. This is correct. A single instance of OpenPages global search server can handle all search requests from all OpenPages application servers.

Q. Can a single search server be shared by multiple environments, such as Development, Testing, Staging, or Production?

A. No. Each environment must have its own OpenPages global search server.

Q. We have two application servers and two Cognos servers for staging and production; do we need to have two global search servers?

A. A single OpenPages global search server works with all OpenPages application servers and Cognos servers. It is strongly recommended to have a separate global search server for staging and production.

Q. Is there a possibility of running global search when using F5 load balancing in an active-active scenario?

A. Because there is only a single instance of OpenPages global search server, there is no need for F5 load balancing.

Q. How does global search impact the database server?

A. During full indexing mode, the database server is used to serve records to the global search indexer. The same is true during incremental indexing mode, but the load on the database is less because only modified records and newly added records are read. When a user uses global search and complex security rules exist for that user, those rules are processed, so the complexity of the rules determines the impact on the database server.

Q. Do we have any metrics for indexing volumes? What is the speed? Do we have any indicative query response times?

A. There are several factors influence the indexing volume and duration. The number of object types and their fields you enabled for global search and the total number of records, as well as the data size in those records in your database, all influence how long it takes to complete the initial full indexing and how large the index size on disk is. Query response time is within seconds for most searches. In some cases, if a user has complex security rules, it's possible a search can take more than several seconds.

High Availability (HA) and Disaster Recovery (DR)

Q. We have two application servers; one acts as an active administration server and the other one is a passive disaster recovery (DR) server. Do the global search servers also need to be active and passive?

A. No. Because there is only one instance of OpenPages global search server, there is no active / passive setup for it.

Q. Indexing can be lost in a DR scenario. In a DR scenario, does global search require reindexing?

A. Yes. This requires you to fully reindex for the global search feature to become available again. However, all other OpenPages functionality continues to work as normal while the global search index is being re-created.

Maintenance

Q. Are there any backup and restore operations to be performed on the global search server?

A. There are no backup and restore requirements for OpenPages global search. However, if you restore the database from a backup, the global search index is now out of sync with the OpenPages database. In this scenario, you must re-create the global search index by first disabling global search, then dropping the index, and then creating the index.

Q. Are there any index optimizations?

A. There is no need to optimize the OpenPages global search index. Apache Solr dynamically and automatically optimizes the index over time. If you perform a bulk update that impacts over 50% of your records and you have many records - hundreds of thousands of records, for example - the automatic index optimization of Apache Solr can take several days to catch up. If you suspect search performance is suffering because of a bulk update, you can force an index optimization from the Apache Solr administration page.

Collecting search diagnostic data

See [“Before you contact IBM OpenPages Support” on page 1105](#).

Chapter 21. Using IBM OpenPages with Watson utilities with Db2 databases

You can use the IBM OpenPages with Watson utilities to back up and restore the OpenPages and Cognos files and configuration data.

Use the utilities that are provided with IBM Db2 to back up and restore databases in IBM OpenPages with Watson.

Db2 and the OpenPages with Watson backup and restore utilities

The backup and restore utilities are installed during the IBM OpenPages with Watson installation.

Use the utilities that are provided with IBM Db2 to back up and restore databases in IBM OpenPages with Watson.

For information about developing a database backup and restore strategy, see the [IBM Db2 documentation](#).

For more information about backing up or restoring, see [“Db2 database backup and restore for OpenPages”](#) on page 690.

Use the following utilities for backing up and restoring the IBM OpenPages environment:

- OpenPages with Watson backup (OPBackup) and restore (OPRestore)

These utilities are used to backup and restore the application. For more information, see [“The OPBackup utility”](#) on page 682.

Users can choose to run a live OPBackup. When you run a live OPBackup, OpenPages services are not stopped on the application server, which allows for maximum uptime of the OpenPages application. By default, OpenPages services are restarted.

- Cognos backup (OPCCBackup) and restore (OPCCRestore)

These utilities are used to back up and restore OpenPages with Watson Cognos files. For more information, see [“Using the Cognos Backup utility”](#) on page 687.

Email notification for backup jobs

You can configure email notification when you complete an IBM OpenPages with Watson application backup or Cognos backup job.

Note:

- Log files for email notification are stored in the logs folder in the following locations. A timestamp is included in the log file names.

- For OPBackup (OpenPages with Watson application backup):

```
<OP_Home>|aurora|bin|logs
```

- For OPCCBackup (Cognos backup):

```
<CC_Home>|tools|bin|logs
```

- Make sure to set rules in your email client to never send emails from the OpenPages with Watson application server to the Spam or Junk mail folders.

Configuring backup job notification

Use this procedure to configure email parameters for IBM OpenPages with Watson and Cognos backup jobs.

Procedure

1. Open a command or shell window and do one of the following.
 - a) For an OPBackup (OpenPages with Watson application backup, navigate to the `op-backup-restore.env` file in the `<OP_HOME>/aurora/bin` directory.
 - b) For a OPCCBackup (Cognos backup), navigate to the `op-cc-backup-restore.env` file in the `bin` directory where `<cc_home>` represents the installation of Cognos.
 - For Microsoft Windows, the back up path is `OPBackup <path-to-back-up-location>`
 - For Linux, the back up path is `OpBackup.sh <path-to-back-up-location>`where `<path-to-back-up-location>` is the full path of the directory where the backed up files are located on the application server. If a file path is not specified, the OPBackup command uses, by default, the backup location specified in the `BACKUP_LOCATION` parameter of the `<OP_Home>|aurora|bin|op-backup-restore.env` file.
2. Open the selected `.env` file in a text editor.
3. Specify a value after the equal sign (=) for the parameters described in the following table and save the `.env` file.

Table 207. Backup email parameters	
Parameter name	Description
BACKUP_EMAIL_NOTIFICATION_SERVER=	The host name of the outgoing mail server.
BACKUP_EMAIL_NOTIFICATION_TO_EMAIL_ID=	The name of recipients that will receive the email notification. Separate email addresses with a comma (,). Note: Do not type a comma after the last email address. Example emailid1@yourdomain.com,emailid2@yourdomain.com
BACKUP_EMAIL_NOTIFICATION_FROM_EMAIL_ID=	The name that will appear as the sender of the notification email in the <code>From:</code> field of the email. The email address is also used as the personal name.
BACKUP_EMAIL_NOTIFICATION_SUCCESS_MSG_FILE=BACKUP_SUCCESS_MSG.txt	The <code>BACKUP_SUCCESS_MSG.txt</code> file is the default file containing the message text that will be used if the OPBackup.cmd completes successfully. You can modify the message text in the <code>BACKUP_SUCCESS_MSG.txt</code> file. The first line of the file is used as the email's subject.

Table 207. Backup email parameters (continued)	
Parameter name	Description
BACKUP_EMAIL_NOTIFICATION_FAIL_MSG_FILE=BACKUP_FAIL_MSG.txt	The BACKUP_FAIL_MSG.txt file is the default file that contains the message text that is used if the OPBackup.cmd fails with errors. You can modify the message text in the BACKUP_FAIL_MSG.txt file as wanted. The first line of the file is used as the email's subject.

Asynchronous background jobs and administrative functions

IBM OpenPages with Watson supports asynchronous execution of processes in the background.

The most common examples of these type jobs are FastMap web-based data import jobs, object resets, and reporting schema generation.

For example, after a user submits a data import file, that file is queued for loading and the import process occurs in the background. Because it is important for asynchronous background jobs to run to completion, certain administrative operations are suspended until all background jobs complete.

By default, the following administrative functions will not start until background jobs are complete:

- OPBackup command
- OPRestore command
- System Administrative Mode (SAM)

Note: To disable the default setting that checks for background jobs before you start **OPBackup** or **OPRestore**, see [“Enabling and disabling asynchronous background processes checking”](#) on page 682.

If asynchronous processes are found, error messages are written to the OPBACKUP restore log.

Example

The following is a sample error log message that occurred when an OPBackup command was initiated while the reporting schema was still being generated.

Note: The .log file name has the format `op_backup_<yyyy_mm_dd_hh_mm_ss>.log`

Where:

`<yyyy_mm_dd_hh_mm_ss>` represents the year_month_day_hour_minute_second. For example:

Windows

`C:\OpenPages\openpages-backup-restore\op_backup_2019_07_26_09_35_42.log`

Linux

`/opt/OpenPages/openpages-backup-restore/op_backup_2019_07_26_09_35_42.log`

Sample error log messages follow.

- For Oracle database environments, a sample error log message might look similar to this text:
 - can-proceed:


```
[exec] declare
[exec] *
[exec] ERROR at line 1:
[exec] ORA-20001: There are existing processes running.
[exec] Please let them finish or terminate them before proceeding.
[exec] ORA-06512: at line 7
[exec]
```

```

- can-proceed:
[exec] declare
[exec] *
[exec] ERROR at line 1:
[exec] ORA-20001: There are existing object reset operations running.
[exec] Please let them finish or terminate them before proceeding.
[exec] ORA-06512: at line 7
[exec]

```

- For IBM Db2 environments, a sample error log message might look similar to this text:

```

- can-proceed:
[exec] ERROR near line 26:
[exec] SQL0438N Application raised error or warning with diagnostic
[exec] text: "There are existing processes running. Please let them
[exec] finish or termi".

- can-proceed:
[exec] ERROR near line 26:
[exec] SQL0438N Application raised error or warning with diagnostic
[exec] text: "There are existing object reset operations running.
[exec] Please let them finish or termi".

```

Enabling and disabling asynchronous background processes checking

By default, IBM OpenPages with Watson does not allow a backup (OPBackup) or restore (OPRestore) operation to start until all asynchronous background jobs are complete.

It is best to run all jobs to completion before you start a backup or restore operation. However, this check can be enabled or disabled as follows.

Procedure

1. Open a command or shell window on the OpenPages with Watson server.
2. Navigate to the `op-backup-restore.env` file in the `<OP_Home>/aurora/bin` directory.
3. Open the `op-backup-restore.env` file in a text editor.
4. Set the `CHECK_BACKGROUND_PROCESSES` parameter in the file to true or false.
Setting the value to true enables the asynchronous background job. If background processes are running, this value prevents OPBackup or OPRestore from starting. True is the default value. false disables the validation check for asynchronous background jobs. OPBackup or OPRestore start even if background processes are running.

The OPBackup utility

OPBackup is the IBM OpenPages with Watson backup utility that backs up the necessary product files and database content on the server where it is run. The OPBackup utility creates a backup file that can be used by the OpenPages restore utility (OPRestore).

When you use the OPBackup utility, the following OpenPages with Watson resources are backed up:

- The OpenPages with Watson application
- The OpenPages with Watson storage folder and its content
- The OpenPages with Watson application environment files

In a horizontal clustered environment, if you run OPBackup on a non-administrative server, the application database is not included in the backup. To include this database in a backup file, run OPBackup on an administrative server.

OPBackup does not back up standard tools by default. If you want to include additional files or directories, you must add them to a manifest file before you run the backup. For more information, see [“Backing up custom files” on page 683](#).

Depending on your configuration, if any asynchronous background jobs are detected, an OPBackup job will exit and possibly display errors (see [“Asynchronous background jobs and administrative functions” on page 681](#)).

You can also configure email notification upon completion of an OPBackup. For details, see [“Email notification for backup jobs” on page 679](#).



Attention: If you have global search enabled, global search must be disabled before running the OPBackup and OPRestore utilities. For more information, see [“Using OPBackup and OPRestore when global search is enabled” on page 653](#).

Backing up custom files

You can include custom files, such as custom JSPs or other files that are specific to your environment, in backups by using a manifest file. A manifest file is a text file that contains the full path name to any directory or file that needs to be included in the backup.

For example, if you want to back up `openpages-ext.jar`, add its full path to the manifest file:

```
/opt/opuser/IBM/OpenPages/aurora/lib/openpages-ext.jar
```

Before you begin

- You must list all of your custom directories and files in a manifest. If you have any questions about the location of your custom data, contact IBM OpenPages Support.
- In a horizontal clustered environment, you must perform this procedure on each application server in the horizontal cluster.

Procedure

1. Log on to the application server.
2. If you have custom JSPs, do the following steps:
 - a) Create a zip file called `solutions-sosa-files.zip` that contains your custom JSPs and related files.

Tip: You can use a different name, but it must follow the convention `*-sosa-files.zip`. Also, you must add it to the `<OP_HOME>/aurora/bin/op-backup.manifest` file. Only `solutions-sosa-files.zip` is backed up and restored by default.
 - b) Put the `solutions-sosa-files.zip` file in the `<OP_HOME>/applications` directory.
 - When you run OPBackup, the zip file is included in the backup.
 - When you run OPRestore, the zip file is restored to `<OP_HOME>/applications` and is also extracted to `<OP_HOME>/wlp-user/shared/apps/op-apps.ear/sosa.war/`
3. Open the `<OP_HOME>/aurora/bin/op-backup.manifest` file in a text editor.
4. Add custom files or directories, other than JSPs, to the `op_backup.manifest` file.

You can specify directories or individual files. For each file or directory, create a new line and type its full path..
5. Save the manifest file using the current location and name.

Running a live OpenPages with Watson backup

A live IBM OpenPages with Watson backup means that the application can continue running while the backup is in progress. The services are not stopped during the backup.

Note: Run live OpenPages with Watson backups during off-peak hours because the backup consumes processing resources.

You might encounter errors such as the following during the database export portion of the live OP backup:

```
[exec] ORA-31693: Table data object "OPENPAGES"."table_name"  
failed to load/unload and is being skipped due to error:  
[exec] ORA-02354: error in exporting/importing data  
[exec] ORA-01555: snapshot too old: rollback segment number #  
with name "rollback_segment_name" too small
```

This might happen if there is a relatively high level of data modification transactional activity on the system during the backup. Run live OP backup when transactional activity is low. If this is not possible or not desirable, or if the error keeps happening, it may be possible to avoid this error by setting UNDO_RETENTION initialization parameter to a higher (possibly much higher) value, at least for the duration of the backup. Setting UNDO_RETENTION to a higher value, may result in a growth of UNDO table space, so it should be done by an experienced database administrator or with the assistance of IBM OpenPages Support.

To use the OpenPages with Watson application backup utility live, you run the OPBackup command with the nosrvrst option. This does the following:

- Backs up OpenPages with Watson application and environment files
- Exports the OpenPages with Watson application database

Procedure

1. Open a command or shell window on the OpenPages with Watson admin application server.
2. Navigate to the <OP_Home>/aurora/bin directory.
3. Type the following backup command:

Windows

```
OPBackup <path-to-backup-location> nosrvrst
```

Linux

```
OPBackup.sh <path-to-backup-location> nosrvrst
```

where:

Windows

<path-to-backup-location> is <oracle_base>\admin\<SID>\dpdump

Linux

<path-to-backup-location> is <oracle_base>/admin/<SID>/dpdump

OpenPages with Watson backed-up content

The backup process creates a ZIP file (.zip) in the <backup-directory-name> directory.

The ZIP file contains the following necessary backed up data files:

- IBM OpenPages with Watson properties files (such as aurora.properties and Server<#>-sosa.properties).
- Application server configuration files for IBM WebSphere.
- The openpages-storage directory.
- Pointers to the database schema dump extracts.

- Files and directories that are listed in the manifest file (such as `solutions-sosa-files.zip`).

The manifest file is `<OP_HOME>/aurora/bin/op-backup.manifest`

Note:

- If a backup file is 4 GB or larger, configure the OPBackup utility to use gzip (GNU zip). Gzip produces an archive with an extension of `.tar.gz`. To view and extract the contents of the archive file, use WinZip 12 (or higher) or WinRAR 3.71 (or higher).
- The OPBackup utility adds a timestamp on the `.zip` and log files it creates.

The ZIP file can be used as a parameter to the OPRestore command to restore the installation-specific OpenPages with Watson files and the database. Each time the OPBackup command is run, a separate ZIP file is created and each data file is identified by a unique name.

The OPBackup log file

The backup process creates a log file, which is identified by a unique name in the `<backup-directory-name>` folder. Each time you run the OPBackup command, a separate log file is generated.

Configuring OPBackup to use GZIP

If a ZIP backup file grows beyond the 4-GB limit of ZIP file capacity, you can configure the OPBackup utility to use gzip (GNU zip). After the file is configured, new backup files will have a `.tar.gz` extension. The OPRestore utility detects if a file is in ZIP or gzip format and processes the file accordingly.

Procedure

- From a command or shell window, navigate to the `op-backup-restore.env` file in the `bin` directory as follows.
 - For Windows, the installation directory is `c:\<OP_Home>\aurora\bin`
 - For Linux, the installation directory is `<OP_Home>/aurora/bin`
- Open the `op-backup-restore.env` file in a text editor of your choice.
- Change the `USE_GZIP_COMPRESSION=` setting from `false` to `true`.

Enabling and disabling storage backup

By default, the IBM OpenPages with Watson backup includes the storage folder and its content. You can disable storage backup by setting the `BACKUP_OP_STORAGE` parameter in the `op-backup-restore.env` file.

Procedure

- Open a command or shell window on the OpenPages with Watson server.
- Navigate to the `op-backup-restore.env` file in the `bin` directory as follows.

Table 208. Installation locations	
Operating system	Installation location
Windows	<code><OP_HOME>\aurora\bin</code>
Linux	<code><OP_HOME>/aurora/bin</code>

- Open the `op-backup-restore.env` file in a text editor of your choice.
- Set the value of the `BACKUP_OP_STORAGE` parameter in the file to one of the following:

Table 209. BACKUP_OP_STORAGE parameter values and their meanings	
If the value is set to...	Then...
true	The storage folder and its content are backed up. This is the default value.
false	The storage folder and its content are not backed up.

5. When finished, save the changes to the file and exit the editor.

The OpenPages with Watson restore utility on the Db2 database

OPRestore is the IBM OpenPages with Watson restore utility that restores the necessary product files on the server from which it was originally run. The OPRestore utility uses a backup file that is created by the OpenPages backup utility (OPBackup).

Prerequisites

Important: Before you run the OPRestore utility, you must restore the IBM Db2 OpenPages database.

The OPRestore tool can be used only on an existing OpenPages database. It cannot be used on a database that does not have an OpenPages schema.

Restoring files

To back up or restore the IBM Db2 databases for IBM OpenPages with Watson, you must use the utilities that are provided with Db2. For more information about the databases in IBM OpenPages with Watson and backing up or restoring them, see [“Db2 database backup and restore for OpenPages”](#) on page 690.

Note: To refresh a test environment, see [“Refreshing a test environment from backup files”](#) on page 736.

As part of the restoration process, the following OpenPages resources are restored:

- If the OpenPages storage folder was backed up, the storage folder and its content are restored.

For information about enabling and disabling storage folder backup, see [“Enabling and disabling storage backup”](#) on page 685.

- The OpenPages application environment files are restored.
- The OpenPages database schema is populated with data restored from backup files.

Depending on your configuration, if any asynchronous background jobs are detected, an OPRestore job might exit and possibly display errors. See [“Asynchronous background jobs and administrative functions”](#) on page 681.

Running the OPRestore command

You can restore a backup using the OPRestore command.

Procedure

1. If you enabled the global search component during backup, recreate your search index so that your search results are synchronized.
 - a) Click **Administration > Global Search**.
 - b) Click **Disable** to disable the global search component.
 - c) Click **Drop** to drop the search indexes.
 - d) Click **Create** to recreate the search indexes.
2. Stop the IBM Cognos service.

3. From a command or shell window, navigate to the `<OP_Home>/aurora/bin` directory.
4. Run the following command:

Windows

```
OPRestore <backup-file-name> <path-to-backup-location>
```

Linux

```
OPRestore.sh <backup-file-name> <path-to-backup-location>
```

Where:

`<backup-file-name>` is the name of the backup file (without the `.zip` or `tar.gz` file extension)

What to do next

Preferences related to the long string text index won't be exported by [“Running the OPBackup command” on page 719](#), and therefore are not restored. You must [“Create a long string index for an Oracle database” on page 747](#) pointing to the database server you are restoring to.

OPRestore log files

The restore process creates a log file identified by a unique name in the `<backup-directory-name>` folder. Each time you run the OPRestore command, a separate log file is created.

Note: Oracle Data Pump log files for database imports are created on the database server.

Using the Cognos Backup utility

OPCCBackup is the Cognos utility that backs up the necessary Cognos files. The OPCCBackup utility creates a backup file that can be used by the Cognos restore utility OPCCRestore.

To back up or restore the IBM Db2 databases for IBM OpenPages with Watson, you must use the utilities that are provided with Db2. For more information about the databases in IBM OpenPages with Watson and backing up or restoring them, see [“Db2 database backup and restore for OpenPages” on page 690](#).

To back up or restore the IBM Db2 databases in the OpenPages application, you must use the utilities that are provided with IBM Db2.

When you use the OPCCBackup utility, the following Cognos resources are backed up.

- Cognos reports
- Branding and environment files

You can configure e-mail notification (with an attached log file) upon the completion of an OPCCBackup. For details, see [“Email notification for backup jobs” on page 679](#).

The OpenPages with Watson file storage directory

By default, `OP_DATAPUMP_DIRECTORY` is the name of the directory used for storing Cognos Content Store database backup files. The path to this directory on the database server varies and depends on how it was defined.

If the `OP_DATAPUMP_DIRECTORY` storage directory does not already exist on the database server, you must run the script to create the directory.

Running the OPCCBackup command

When you use the Cognos backup utility, you run the OPCCBackup command in a command or shell window. The OPCCBackup command uses Oracle Data Pump to export the database (services can continue to run during the backup).

Note: Oracle Data Pump backup files are created on the database server.

Procedure

1. From a command or shell window, navigate to the `<CC_Home>/tools/bin`, where `<CC_Home>` represents the installation location of the Cognos application.
2. Run the following backup command:

Windows

```
OPCCBackup <path-to-backup-location>
```

Linux

```
OPCCBackup.sh <path-to-backup-location>
```

Where:

`<path-to-backup-location>` is the full path of the directory where the backed up files are located on the Cognos server. The file path is optional.

Note: If no file path is specified, the OPCCBackup command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the `<CC_Home>/tools/bin/op-cc-backup-restore.env` file.

The following table lists the default content store database export location specified in the environment file.

Where `<SID>` is the Oracle System Identifier (for example, OP).

The default content store database export locations are:

Windows: `<oracle_base>\admin\<SID>\dpdump`

Linux: `<oracle_base>/admin/<SID>/dpdump`

If you get the warning `tools.jar file is not found`, see the following [technote](#).

The OPCCBackup log file

The backup process creates a log file, which is identified by a unique name in the `<backup-directory-name>` folder. Each time you run the **OPCCBackup** command, a separate log file is generated.

Cognos backed-up content

The Cognos backup process creates a ZIP file (.zip) in the `<backup-directory-name>` directory. This ZIP file contains the necessary report and environment files that can be used by the Cognos restore utility (OPCCRestore).

Note:

- If a backup file is very large (4 GB or larger), configure the OPCCBackup utility to use gzip (GNU zip). Gzip produces an archive with an extension of `.tar.gz`. To view and extract the contents of the archive file, use WinZip 12 (or higher) or WinRAR 3.71 (or higher).
- The OPCCBackup utility adds a military timestamp on the .zip and log files it creates.

The ZIP file can be used as a parameter to the OPCCRestore command to restore the installation-specific IBM OpenPages with Watson files and the database. Each time the OPCCBackup command is run, a separate ZIP file is created and each data file is identified by a unique name.

Configuring OPCCBackup to use GZIP

If a ZIP backup file grows beyond the 4-GB limit of ZIP file capacity, you can configure the OPCCBackup utility to use gzip (GNU zip). After the file is configured, new backup files will have a `.tar.gz` extension. The OPCCRestore utility will detect if a file is in ZIP or gzip format and process it accordingly.

Procedure

1. From a command or shell window, navigate to the `op-cc-backup-restore.env` file in the `bin` directory as follows, where `<CC_Home>` represents the installation location of the Cognos application..
 - For Microsoft Windows, the `bin` directory is `<CC_Home>\tools\bin`. By default, `<CC_Home>` is `C:\OpenPages\CommandCenter`.
 - For Linux, the `bin` directory is `<CC_Home>/tools/bin`. By default, `<CC_Home>` is `opt/OpenPages/CommandCenter`.
2. Open the `op-cc-backup-restore.env` file in a text editor.
3. Change the **USE_GZIP_COMPRESSION=** setting in the file from `false` to `true`.

Using the Cognos Restore utility

OPCCRestore is the IBM OpenPages with Watson Cognos utility that restores the necessary Cognos files on the server from which it was originally run. The OPCCRestore utility uses a backup file created by the OPCCBackup utility.

Important: Before you run the OPCCRestore utility, you must restore the IBM Db2 reporting database.

To back up or restore the IBM Db2 databases for IBM OpenPages with Watson, you must use the utilities that are provided with Db2. For more information about the databases in IBM OpenPages with Watson and backing up or restoring them, see [“Db2 database backup and restore for OpenPages”](#) on page 690.

As part of the OPCCRestore restoration process, the following Cognos resources are restored:

- Cognos reports
- Branding and environment files

For information about refreshing a test environment, see [“Refreshing a test environment from backup files”](#) on page 736.

Running the OPCCRestore command

You can restore backed up Cognos data using the OPCCRestore utility as follows.

Procedure

1. Stop the Cognos service on the administrative server and any non-administrative servers in the cluster. For details, see [“Starting and stopping the Cognos services”](#) on page 849.
2. Stop the IBM Cognos Configuration tool, if it is running, on all cluster members.
3. From a command or shell window, navigate to the `bin` directory as follows:

Where `<CC_HOME>` represents the installation location of the Cognos application.

Table 210. Installation location of the Cognos application	
Operating system	Installation location
Windows	<code><CC_HOME>\tools\bin</code> By default, <code><CC_HOME></code> is <code>C:\IBM\OpenPages\CommandCenter</code>
Linux	<code><CC_HOME>/tools/bin</code> By default, <code><CC_HOME></code> is <code>/opt/IBM/OpenPages/CommandCenter</code>

4. On the administrative Cognos server, execute the following command:

Windows

```
OPCCRestore <backup-file-name> <path-to-backup-location>
```

Linux

```
OPCCRestore.sh <backup-file-name> <path-to-backup-location>
```

Where:

<backup-file-name> is the name of the backup file (without the .zip or tar.gz file extension).

Note: <path-to-backup-location> is the full path of the directory where the backed up files are located on the Cognos server. The file path is optional.

Note: If no file path is specified, the OPCCRestore command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the <CC_Home>|tools|bin|op-cc-backup-restore.env file.

5. Start the Cognos service on the administrative server and on any non-administrative servers in the cluster. For details, see [“Starting and stopping the Cognos services”](#) on page 849.

The OPCCRestore log file

The restore process creates a log file identified by a unique name in the <backup-directory-name> folder.

Each time you run the OPCCRestore command, a separate log file is created.

Db2 database backup and restore for OpenPages

You must use the utilities that are provided with IBM Db2 to back up and restore Db2 databases for OpenPages.

Note: This task applies to OpenPages with Watson. For information about backing up external databases for IBM OpenPages for IBM Cloud Pak for Data, see [Backing up, restoring, and migrating OpenPages](#).

For information about developing a backup and restore strategy, see the [IBM Db2 documentation](#).

Db2 databases in OpenPages

There are two databases in IBM OpenPages with Watson that require backup:

- The OpenPages with Watson database

This database is the main application database that is created in the Db2 instance with Oracle Compatibility mode enabled.

- The IBM Cognos Controller database

This database is created in another normal Db2 instance without the Oracle Compatibility feature.

In IBM OpenPages for IBM Cloud Pak for Data, there is one database to back up: the OpenPages database.

OpenPages Db2 database backup

For IBM OpenPages with Watson, to do a complete backup of the IBM OpenPages with Watson and the IBM Cognos Controller databases, you must back up each database from each of their instances. The best approach is to do an offline backup of your Db2 databases.

For IBM OpenPages for IBM Cloud Pak for Data, do an offline backup of the external database.

1. Make sure that no OpenPages services are running for any long running background processes (such as, object reset jobs).
2. Stop the OpenPages services:

OpenPages with Watson

Stop the OpenPages with Watson servers. For information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.

IBM OpenPages for IBM Cloud Pak for Data

Do steps 1-3 in [“Performing an offline backup”](#) on page 49.

3. Open a command or shell window and connect to the Db2 database as the database instance owner.

For Windows users only, you must use the **db2cmd** command in the **Command Prompt** window to initialize the Db2 command line processor (CLP).

4. Start the Db2 instance by using the **db2start** command.
5. Do the offline backup.

For example, on a Linux operating system, to back up a database with the alias name of `sample` to `/opt/db2backup`, you can use `db2 backup db sample /opt/db2backup`. A backup image is created in the specified backup location in the following format:

database_name.backup_type.instance_name.database_partition.catalog_partition_number.backup_date_time.time_image_sequence_number. For example, `OPX.0.DB2INST1.NODE0000.CATN0000.20121129.131259.001`.

On a Microsoft Windows operating system, to back up a database with the alias name of `sample` to `c:\Db2backup`, you can use `db2 backup db sample c:\Db2backup`. A backup image is created in the specified backup location in the following format:

database_name.backup_type\instance_name\database_partition\catalog_partition_number\backup_date_time\time_image_sequence_number. For example, `OPX.0\DB2INST1\NODE0000.\CATN0000\20121129\131259.01`.

For information about backing up your Db2 database, see the [IBM Db2 documentation](#).

6. Start the OpenPages services:

OpenPages with Watson

Start the OpenPages with Watson servers. For information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.

IBM OpenPages for IBM Cloud Pak for Data

Do steps 13-15 in [“Performing an offline backup”](#) on page 49.

OpenPages Db2 database restore

You can use a Db2 database backup from your production system to restore a Db2 database to a previous state in the same environment.

Use this process as a guide for restoring a OpenPages Db2 database:

1. Stop the OpenPages services:

OpenPages with Watson

Stop the OpenPages with Watson servers. For information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.

IBM OpenPages for IBM Cloud Pak for Data

Do steps 1-3 in [“Restoring IBM OpenPages for IBM Cloud Pak for Data”](#) on page 52.

2. Open a command or shell window and connect to the Db2 database as the database instance owner.

For Windows users only, you must use the **db2cmd** command in the **Command Prompt** window to initialize the Db2 command line processor (CLP).

3. Restore the Db2 database.

For example, on a Linux operating system, to restore a database with the alias name of `sample` from the backup location `/opt/db2backup` with a backup timestamp of `20121129131259`, you can use `db2 restore db sample from /opt/db2backup taken at 20121129131259`.

On a Windows operating system, to restore a database with the alias name of `sample` from the backup location `c:\Db2backup` with a backup timestamp of `20121129131259`, you can use `db2 restore db sample from c:\Db2backup taken at 20121129131259`.

For information about restoring your Db2 database, see the [IBM Db2 documentation](#).

4. Start the OpenPages services:

OpenPages with Watson

Start the OpenPages with Watson servers. For information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.

IBM OpenPages for IBM Cloud Pak for Data

Do steps 16-18 in [“Restoring IBM OpenPages for IBM Cloud Pak for Data”](#) on page 52.

Moving a database when you can't use backup and restore

In some cases, it is not possible to move a Db2 database between OpenPages with Watson environments by doing a backup and restore. For example, Db2 does not support using a backup and restore to move a database if the source and target environments are using different operating systems or if the source and target are using different schema names. For more information, see [Backup and restore operations between different operating systems and hardware platforms](#) in the Db2 documentation.

Db2 has several tools and techniques that you can use instead. For more information about how to use these tools with OpenPages, see [Moving Db2 database objects to a new database when a backup and restore cannot be performed](#).

Restoring backed up production data in a new Db2 environment

You can use a IBM Db2 database backup from your production environment to restore data to a Db2 database in a new test or development environment.

The process of restoring data involves the following tasks in this order:

1. Back up your Db2 production databases then restoring these databases to the new environment.

When you create the IBM OpenPages with Watson application database, you must run scripts to enable Oracle compatibility and update configuration data. You run these scripts before you restore the OpenPages with Watson application production database to the new environment. These scripts are not required for the Cognos database.

2. Back up your production application and reporting data files then restore these files to the new environment.

3. Update the storage folder location in the new environment.

For information about refreshing a test environment on an existing test system, see [“Refreshing a test environment from backup files \(Db2\)”](#) on page 694.

Before you begin

Make sure that your new test or development environment meets the following prerequisites:

- OpenPages with Watson is installed in the new test or development environment.
- The operating system user names in the new environment match the operating system user names in your production environment.

Procedure

1. Back up your OpenPages with Watson application production Db2 database.
For more information, see [“OpenPages Db2 database backup”](#) on page 690.
2. Back up your IBM Cognos Controller production Db2 database.
For information about backing up the IBM OpenPages application database, see [“OpenPages Db2 database backup”](#) on page 690.
3. Create the OpenPages with Watson application database instance in the new environment.
For more information about creating a Db2 database, see the IBM Db2 documentation.

4. On the new OpenPages with Watson application database only, run the `enable-ora-compatibility` script to enable Oracle Compatibility Mode.
In the output, look for the Db2 profile variable, **DB2_COMPATIBILITY_VECTOR**, with the value of ORA. For example, **DB2_COMPATIBILITY_VECTOR=ORA**.

Microsoft Windows

- a. Click **Start > IBM Db2 > DB2COPY1 > Command Window - Administrator**.

Note: If you have multiple instances of Db2 on the server, make sure that you choose the DB2COPY of the OpenPages database instance.

- b. Run the following command: **enable-ora-compatibility.bat**

Linux

Run the following command: **./enable-ora-compatibility.sh**

Note: Db2 compatibility features are enabled at the instance level and cannot be disabled. Keep the selected compatibility level for the life of the OpenPages database. To confirm that Oracle Compatibility Mode is set, type the following command: **db2set -all**

5. On the new IBM OpenPages application database only, update the database manager configuration.
 - a) For Windows users only, type the following command in the **Command Prompt** window to initialize the Db2 command line processor (CLP):

db2cmd

- b) In the Db2 CLP, run the `opx-dbm-cfg` script:

- On Windows, type:

`opx-dbm-cfg.bat`

- On Linux, type:

`./opx-dbm-cfg.sh`

6. Use the OpenPages with Watson application database backup from your production system to restore the Db2 database to your new environment.

For more information, see [“OpenPages Db2 database restore”](#) on page 691.

7. Create the IBM Cognos Controller database instance in the new environment without the Oracle Compatibility feature.

For more information about creating a Db2 database, see the IBM Db2 documentation.

8. Use the IBM Cognos Controller database backup from your production system to restore the Db2 database to your new environment.

For more information, see [“OpenPages Db2 database restore”](#) on page 691.

9. Use the OpenPages with Watson backup and restore utilities to back up the product files on the production server then restore these files to your new environment.

For more information about using the OpenPages with Watson backup utility, see [“The OPBackup utility”](#) on page 682.

For more information about using the OpenPages with Watson restore utility, see [“The OpenPages with Watson restore utility on the Db2 database”](#) on page 686.

10. Use the Cognos backup and restore utilities to back up your reporting files on the production server then restore these files to your new environment.

For more information about using the Cognos backup utility, see [“Using the Cognos Backup utility”](#) on page 687.

For more information about using the Cognos restore utility, see [“Using the Cognos Restore utility”](#) on page 689.

11. Update the OpenPages storage folder location on the new test or development database.

For more information about updating the storage folder location, see [“Update the OpenPages with Watson storage location in the Db2 database”](#) on page 696.

Refreshing a test environment from backup files (Db2)

The best method for refreshing an existing test environment is to have it replicated from the production environment. By using your production environment's backup files, you can update a test environment that closely matches your production environment as of the backup date.

You can use this procedure to refresh a test server by using the backup files from another IBM OpenPages with Watson server.

Prerequisites:

- Make sure that you have access to both the production or "source" and test or "target" servers.
- The operating systems must match between the source and target servers.
- The OpenPages version and patch level must match between the source and target servers.

Prerequisites to refreshing a Db2 test environment

There are some prerequisites to refreshing a test environment.

The following are required:

- The test or "target" server and production or "source" server must have the same installed version of the IBM OpenPages with Watson application - including patches.
- You must have access to the OpenPages with Watson installation files.

Backup of production databases in OpenPages with Watson on the Db2 server

You must use the utilities that are provided with IBM OpenPages with Watson to back up the production databases in the application. The exported IBM Db2 production databases are used later to refresh the OpenPages with Watson application databases on the test or target server.

For more information about the databases in OpenPages with Watson and backing up Db2 databases, see [“Db2 database backup and restore for OpenPages”](#) on page 690.

Backing up and copying OpenPages with Watson application production files for a Db2 database

The IBM OpenPages with Watson backup utility backs up the application files. The exported data from the production backup file is used later to refresh data on the test or target server.

Procedure

1. Log on to your production OpenPages with Watson server as a user with administrative permissions.
2. Run the OpenPages with Watson backup utility (OPBackup) to back up the application files.
For more information, see [“The OPBackup utility”](#) on page 682.
3. Copy the backup .zip or .tar.gz file to your test server.

Backup of OpenPages with Watson databases on the test server

You must use the utilities that are provided with IBM Db2 to back up the test or target databases in IBM OpenPages with Watson.

For more information about the databases in OpenPages with Watson and backing up Db2 databases, see [“Db2 database backup and restore for OpenPages”](#) on page 690.

Backing up OpenPages with Watson application files on your test server

Run the IBM OpenPages with Watson backup utility to back up the application files on your test or target server.

Procedure

1. Log on to your test OpenPages with Watson server as a user with administrative permissions.
2. Run the backup utility (OPBackup) as described in [“The OPBackup utility” on page 682](#) to backup the OpenPages with Watson application files.

Running the OPCCBackup command

When you use the Cognos backup utility, you run the OPCCBackup command in a command or shell window.

Procedure

1. From a command or shell window, navigate to the bin directory as follows:

For Microsoft Windows:<CC_Home>\tools\bin By default, <CC_Home> is
C:\OpenPages\CommandCenter

For Linux, type <CC_Home>/tools/bin By default, <CC_Home> is /opt/OpenPages/
CommandCenter

2. Execute the following backup command:

Windows: OPCCBackup <path-to-backup-location>

Linux: OPCCBackup.sh <path-to-backup-location>

Where:

<path-to-backup-location> is the full path of the directory where the backed up files are located on the Cognos server. The file path is optional.

Note: If no file path is specified, the OPCCBackup command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the <CC_Home>|tools|bin|op-cc-backup-restore.env file.

Drop the Db2 database for the application on the test system

You must drop the IBM OpenPages with Watson database on the test server. Dropping the IBM Db2 database for IBM OpenPages with Watson on the test system deletes all object data.

The Db2 database includes OpenPages with Watson application data.

Procedure

1. Log on to your IBM OpenPages with Watson test server as a user with administrative permissions.
2. Stop all OpenPages, Cognos, and global search services.
3. Open a command or shell window.
4. For Windows users only, type the following command in the **Command Prompt** window to initialize the Db2 command line processor (CLP):

db2cmd

5. In the Db2 CLP, type the following command to drop the Db2 test database:

db2 drop db <DATABASE_NAME>

Where <DATABASE_NAME> is the name of the test database.

For example, if the name of the test database is op, type db2 drop database op.

Copy and restore the production Db2 database backup file to the test Db2 database server

You must use the utilities that are provided with IBM Db2 to restore the IBM OpenPages with Watson database on the test system.

Before you begin

The operating system user names in the test environment must match the operating system user names in your production environment.

Procedure

1. Copy the OpenPages with Watson database backup file from the Db2 production server to the test database server.
2. Copy the Java UDF class files from the Db2 production server folders to the folders on the test database server.
For example:
 - On Windows systems, copy the class files from C:\IBM\SQLLIB\FUNCTION on the production database server to the Db2 database server on the test system.
 - On Linux systems, copy the class files from /home/db2inst1/sqllib/function on the production database server to the Db2 database server on the test system.
3. Restore the Db2 database to the test server. For more information, see [“OpenPages Db2 database restore”](#) on page 691.

Update the OpenPages with Watson storage location in the Db2 database

After you restore the openpage-storage files from the production backup, you must update the IBM OpenPages with Watson storage location on the test database.

Procedure

1. Log on to a system as a user with administrator privileges. You can use any system with access to CLPPlus that can connect to the OpenPages database server.
2. Copy all the files under the openpages-storage folder from the production backup .zip file to the openpages-storage location on the test server.

By default, the storage location is <OP_Home>\openpages-storage.

Table 211. Installation location of the OpenPages with Watson application	
Operating system	Installation location
Windows	For example, <OP_Home> C:\IBM\OpenPages
Linux	For example, <OP_Home> /opt/IBM/OpenPages

3. Open a command or shell window and do the following tasks:
 - a) Go to the INSTALL_SCRIPTS directory in the installation package:
/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS
4. For Windows users only, type the following command in the **Command Prompt** window to initialize the Db2 command line processor (CLP):
db2cmd
5. From the INSTALL_SCRIPTS directory, run the update-storage SQL wrapper script with the following parameters to update the openpages-storage directory location in the database:

- On Windows:

```
clpplus -nw <op_db_user>/\ '<op_db_password>'@<database_host>:
<database_port>/<database_name> @sql-wrapper update-storage <log-file>
<database_host> <database_port> <database_name> <op_db_user> '\ '<op_db_password>' <storage-
type> <storage-server-name> <host-name> Windows <path-or-UNC-name>
```

- On Linux:

```
clpplus -nw <op_db_user>/\ '<op_db_password>\ '@<database_host>:
<database_port>/<database_name> @sql-wrapper update-storage <log-file>
<database_host> <database_port> <database_name> <op_db_user> \ '<op_db_password>\ '
<storage-type> <storage-server-name> <host-name> Unix <path-or-UNC-name>
```

Table 212. Update Storage Wrapper Script Parameters

Parameter	Description
<i>op_db_user</i>	The OpenPages user name for accessing the OpenPages database.
<i>op_db_password</i>	The password of the <i>op_db_user</i> user.
<i>database_host</i>	The host name of the Db2 server that contains the OpenPages database.
<i>database_port</i>	The port number of the Db2 database instance that is installed on the database server. For Db2, the default port is 50000.
<i>database_name</i>	The name of the OpenPages database.
<i>log-file</i>	The name of the log file that the script creates and writes information to.
<i>storage-type</i>	The type of file storage to be used. Valid values are as follows: • LFS (local file system) • UNC (Universal Naming Convention) - for Windows only. Note: After you move from LFS to UNC, you cannot go back to using LFS.
<i>storage-server-name</i>	The name of the storage server.
<i>host-name</i>	The host name of the machine.
<i>os-type</i>	The type of operating system. Valid values are as follows: • Windows • Unix
<i>path-or-UNC name</i>	The file path of the storage location.

Examples

- LFS (Linux) :

```
clpplus -nw openpage/\ 'password\ '@myserver:50000/OPX @sql-wrapper
update-storage log.log myserver 50000 OPX openpage \ 'password\ ' LFS server1 server1 Unix /
home/opuser/OP/OpenPages/openpages-storage
```

- LFS (Windows):

```
clpplus -nw openpage/'password'@myserver.ibm.com:50000/OPX @sql-wrapper update-storage
log.log myserver.ibm.com 50000 OPX openpage 'password' LFS server1
server1 Windows C:\openpages-storage
```

- UNC (Windows):

```
clpplus -nw openpage/'password'@myserver.ibm.com:50000/OPX @sql-wrapper update-storage
log.log myserver.ibm.com 50000 OPX openpage 'password' UNC server1
server1 Windows openpages-storage
```

Back up the Cognos database on the Db2 production and test servers

You must use the utilities that are provided with IBM Db2 to back up the IBM Cognos Controller database on both the production and test servers. The exported Db2 production database is used later to refresh the IBM Cognos Controller database on the test or target server.

For more information about the databases in IBM OpenPages and backing up Db2 databases, see [“Db2 database backup and restore for OpenPages”](#) on page 690.

Back up Cognos configuration files on the Db2 production and test servers

You must run the Cognos backup utility to back up Cognos configuration files on both the production and test servers. The Cognos configuration file backup from the production server is used later to refresh Cognos configuration on the test server.

Before you begin

Before you run the Cognos backup utility (OPCCBackup) make sure to verify the following:

- You have access to both the source and target database servers.
- Full permission is granted to the CommandCenter\tools\bin folder on the target Cognos server.

Procedure

1. If necessary, log on to your production Cognos server as a user with administrative permissions.
2. Run the Cognos backup utility (OPCCBackup) to back up the Cognos configuration files on the production server.

For more information, see [“Using the Cognos backup utility”](#) on page 724.

Tip: If the mail server for notification email is not set up for running Cognos backups, the output from the OPCCBackup command might end with the following error:

```
BUILD FAILED
c:\machine3\CommandCenter\tools\bin\op-cc-backup-email-notification.xml:31:
Problem while sending mime mail:
```

This error can be safely ignored if the step before the error says BUILD SUCCESSFUL.

3. Copy the production Cognos server backup .zip or .tar.gz file to the Cognos backup-restore directory on the test server.
4. Run the Cognos backup utility (OPCCBackup) to back up the Cognos configuration files on your test server.

For more information, see [“Using the Cognos backup utility”](#) on page 724.

Modify SSO and LDAP configuration in the test environment

If you are using SSO or LDAP in the test environment, modify the configuration for each if needed. Otherwise, skip this task.

Copy and restore the Cognos production database backup file to the test database server

You must use the utilities that are provided with IBM Db2 to restore the IBM Cognos Controller reporting database on the test system.

Before you begin

The operating system user names in the test environment must match the operating system user names in your production environment.

Procedure

1. Copy the IBM Cognos Controller database backup file from the Db2 production server to the test database server.
2. Restore the Db2 database to the test server. For more information, see [“OpenPages Db2 database restore”](#) on page 691.

Drop the Db2 database for Cognos on the Test Server

You must drop the IBM Cognos Controller database on the test server. Dropping the IBM Cognos Controller database on the test system deletes all object data.

Procedure

1. Log on to your IBM OpenPages with Watson test server as a user with administrative permissions.
2. Stop all OpenPages, Cognos, and global search services.
3. Open a command or shell window.
4. For Windows users only, type the following command in the **Command Prompt** window to initialize the Db2 command line processor (CLP):

db2cmd

5. In the Db2 CLP, type the following command to drop the Db2 test database:

```
db2 drop db <DATABASE_NAME>
```

Where <DATABASE_NAME> is the name of the test database.

For example, if the name of the test database is op, type `db2 drop database op`.

Copy custom deliverables to the test environment

If you are using custom deliverables, you must copy any custom files to the test environment.

Copy custom triggers

You must copy any custom Java actions and triggers that have been deployed on the production server to the test environment. These custom actions and triggers are added to a zip file, `openpages-ext.jar`, by the OPBackup utility.

If you have any questions about the location of your custom data, contact IBM OpenPages Support.

Procedure

1. If necessary, log on to your test IBM OpenPages with Watson server as a user with administrative permissions.
2. Update the `openpages-ext.jar` in the test environment as follows:
 - a) From the production backup .zip file, navigate to the `openpages-ext.jar` in the `<OP_Home>|aurora|lib` directory.

Where `<OP_HOME>` represents the installation location of the IBM OpenPages application.

Table 213. Installation location of the OpenPages with Watson application	
Operating system	Installation location
Windows	<code><OP_HOME>\aurora\lib\openpages-ext.jar</code> By default <code><OP_HOME></code> is <code>C:\IBM\OpenPages</code>

Table 213. Installation location of the OpenPages with Watson application (continued)	
Operating system	Installation location
Linux	<OP_HOME>/aurora/lib/openpages-ext.jar By default <OP_HOME> is /opt/IBM/OpenPages

- b) Copy the openpages-ext.jar from the production backup file into the <OP_Home>|aurora|lib directory on your test machine and overwrite the existing .jar file there.

Copy other custom deliverables to the test environment

If you have other custom deliverables, such as UI helpers and JSP reports, copy these custom deliverables to their respective folders on the test or target machine.

If you have any questions about the location of your custom data, contact IBM OpenPages Support.

Procedure

1. From your application production backup .zip files, extract all custom files such as JAR files, JSP files, JavaScript files, and Image files.
2. Copy these files into their respective folders on the target machine. The target folders should match the folders on the source installation.

Starting the OpenPages with Watson in the test environment

When finished, start IBM OpenPages with Watson services on the servers in your test environment.

For details, see [Chapter 24, “Starting and stopping servers,” on page 841](#).

Updating the OPSysSystem password

If the OPSysSystem password is different in the source (production) and target (test) environments or if you changed the default OPSysSystem password, update the OPSysSystem password in the test environment.

For more information, see [“Changing the OPSysSystem password” on page 773](#).

Update Db2 database connection references for Cognos

You must update the database connection references for the server on the IBM Cognos Analytics.

Procedure

1. From a browser, log on to the IBM Cognos Analytics as a user with administrative privileges, for example, OpenPagesAdministrator.

By default, the URL is `http://<hostname>/ibmcognos/bi`

Where <hostname> is the name of the Cognos server.

2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Configuration** tab, click **Data Source Connections** (if not already selected).
4. On the **Directory > Cognos** page, click the link for the OpenPages DataSource.
5. On the **Directory > Cognos > OpenPages DataSource** page, do the following:

- a) Under the **Actions** column, click the **Set properties - OpenPages DataSource** icon .
- b) On the **Set properties - OpenPages DataSource** page, click the **Connection** tab.

6. On the **Connection** tab, next to the **Connection String** box, click the pencil icon to edit the field.

7. On the **CLI** tab, in the **DB2 database name** box, change the Db2 database name to the Catalog Database Name of the OpenPages with Watson database on the target environment.
8. On the **JDBC** tab, in the **Server name**, **Port number**, and **Database name** boxes, change the values to valid values for the OpenPages with Watson database on the target environment.

Update URL host pointers for Cognos reports

Modify the URL host pointer settings and then propagate these changes to the reporting schema on the application server (does not require services to be restarted).

For more information, see [“Updating URL host pointers for reports” on page 769](#).

Update the global search settings

After you import data from a production environment (the source environment) into a test or development environment (the target environment), you need to update the global search settings.

About this task

When you import data from the source environment, the settings for the search server are imported. You need to update the target environment so that it uses the search server in your target environment.

Procedure

1. Log in to the OpenPages application in the target environment as a user with administrative privileges.
2. If the global search component is enabled, disable it.
 - a) Click **Administration > Global Search**.
 - b) Click **Disable**.
3. Stop the global search services.

For more information, see [“Start or stop the global search services” on page 844](#).

4. Update the global search settings.
 - a) Click **Administration > Settings > Applications > Common > Configuration > Show Hidden Settings** and set the value to **true**.
 - b) Click **Administration > Settings > Platform > Search > Admin** and update the **Search Server Administration URL** with the URL of the search server in your target environment.
 - c) Click **Administration > Settings > Platform > Search > Index** and update the **Search Server URL** with the URL of the search server in your target environment.
 - d) Click **Administration > Settings > Platform > Search > Request** and update the **Search Server URL** with the URL of the search server in your target environment.
5. Copy the `<SEARCH_HOME>/openpages-solr-index` directory to the search server in the target environment.

The `<SEARCH_HOME>/openpages-solr-index` contains the global search index.

6. Start the global search services.

For more information, see [“Start or stop the global search services” on page 844](#).

7. Enable global search. Click **Administration > Global Search > Enable**.

Results

Global search is enabled in the target environment.

Utilities for filtering on long string field content in a Db2 database

You can filter based on the content of long string fields if the IBM Db2 Text Search feature is enabled. This feature is also known as full text searching.

The Db2 Text Search feature is installed and configured during the IBM OpenPages with Watson installation process. For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.



Warning: Do not include long string fields that are encrypted using field level encryption in the search criteria because they can return unexpected results.

Long string fields allow users to enter values over 4 KB in length. For information about setting up long text fields, see [“Long String data type” on page 204](#).

You can do the following tasks to manage full text searching:

- [“Create a long string index in a Db2 database” on page 703](#)
- [“Change the scheduled job that synchronizes the long string index in the database \(Db2\)” on page 705](#)
- [“Drop a long string index” on page 707](#)
- [“Enable Db2 text search” on page 702](#)

For information about how to disable Db2 text search, see [Disabling a database for Db2 Text Search](#).

To apply filters with long string fields, you must change the **Platform > Database > Text Indexes** setting to **true**.

If the value is set to true, filtering is enabled on long string fields. The default value is false.

For details on working with settings, see [Chapter 19, “Viewing the Configuration and Settings page,” on page 597](#).

Enable Db2 text search

Enable the IBM Db2 Text Search feature to filter based on the contents of fields with long string data types.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to CLPPlus that can connect to the IBM OpenPages with Watson database server.

Note: For SQL tool information, see [“Database tool information” on page xxxi](#).

2. Open a command or shell window, navigate to the text-indexing directory as follows:

Windows

```
<OP_HOME>\aurora\bin\full-text-index
```

Linux

```
<OP_HOME>/aurora/bin/full-text-index
```

Note: If the database server is not on the same machine as the IBM OpenPages application server, you must copy the script and the SQL files that the script invokes to the database server.

3. Run the following SQL script:

```
clpplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql  
<LOG_FILE_NAME> <DB2_SERVER_NAME> <DB2_PORT_NUMBER> <DATABASE_NAME>  
<DB2_INSTANCE_OWNER_NAME> <DB2_INSTANCE_OWNER_PASSWORD> <OP_DB_USER>
```

Table 214. Enable Db2 Text Search required script parameters

Required Parameter	Description
<LOG_FILE_NAME>	Name of the log file.

Table 214. Enable Db2 Text Search required script parameters (continued)	
Required Parameter	Description
<DB2_SERVER_NAME>	Name of the Db2 server.
<DB2_PORT_NUMBER>	Port number of the Db2 database service
<DATABASE_NAME>	Name of the OpenPages database.
<DB2_INSTANCE_OWNER_NAME>	Database instance owner account. Usually db2admin user.
<DB2_INSTANCE_OWNER_PASSWORD>	Password for instance owner account. If the password contains special characters, surround the password in quotation marks: • Windows: "password" • Linux: 'password'
<OP_DB_USER>	OpenPages user name for accessing the OpenPages database.

For example:

- Windows:

```
clpplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql
CustomIndexing_Step1_AddTextIndexing_to_DB.log server1 50000 op1 db2admin
"password" OPENPAGES
```

- Linux:

```
clpplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql
CustomIndexing_Step1_AddTextIndexing_to_DB.log server1 50000 op1 db2admin
'password' OPENPAGES
```

Results

The database is now enabled for indexing. Use [“Create a long string index in a Db2 database” on page 703](#) script to create the index.

Create a long string index in a Db2 database

Create a long string text index to support filtering based on the contents of fields with long string data types. Scripts are provided for Microsoft Windows and Linux.

Important: In Linux operating systems, when using asterisks (*) as parameter values in long string search scripts, the asterisks must be properly escaped with a double quote, single quote combination: ""*"".

Before you begin

Complete the following tasks:

- [“Enable Db2 text search” on page 702](#).
- Ensure that the Db2 text search server information is set up.

For more information, see [Updating Db2 Text Search server information](#).

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to CLPPlus that can connect to the IBM OpenPages with Watson database server.

Note: For SQL tool information, see [“Database tool information”](#) on page xxxi.

2. Open a command or shell window, navigate to the text indexing directory as follows.

The following table identifies the installation location of the application on the Microsoft Windows and Linux operating systems.

Table 215. Installation location of the full-text-index directory	
Operating system	Installation location
Windows	<OP_HOME>\aurora\bin\full-text-index
Linux	<OP_HOME>/aurora/bin/full-text-index

Note: If the database server is not on the same machine as the IBM OpenPages application server, you must copy the script and the SQL files that the script invokes to the database server.

3. Run the following script:

```
clpplus -nw @sql-wrapper CustomIndexing_Step2_IndexCreate.sql  
<LOG_FILE_NAME> <DB2_SERVER_NAME> <DB2_PORT_NUMBER> <DATABASE_NAME>  
<OP_DB_USER> <OP_DB_PASSWORD> <UPDATE_FREQUENCY_WEEKDAY>  
<UPDATE_FREQUENCY_HOUR> <UPDATE_FREQUENCY_MINUTE> <MINIMUM_UPDATES>
```

Table 216. Create Db2 long string index required script parameters	
Required Parameter	Description
<LOG_FILE_NAME>	Name of the log file.
<DB2_SERVER_NAME>	Name of the Db2 server.
<DB2_PORT_NUMBER>	Port number of the Db2 database service
<DATABASE_NAME>	OpenPages database name.
<OP_DB_USER>	OpenPages user name for accessing the OpenPages database.
<OP_DB_PASSWORD>	OpenPages password for accessing the OpenPages database. If the password contains special characters, surround the password in quotation marks: • Windows: "password" • Linux: 'password'
<UPDATE_FREQUENCY_WEEKDAY>	Weekday update frequency. Accepted values are between 0 and 6; multiple values can be separated with a comma. For all weekdays use * (asterisk).

Table 216. Create Db2 long string index required script parameters (continued)	
Required Parameter	Description
<UPDATE_FREQUENCY_HOUR>	Hourly update frequency. Accepted values are between 0 and 23; multiple values can be separated with a comma. For all hours use * (asterisk).
<UPDATE_FREQUENCY_MINUTE>	Minute update frequency. Accepted values are between 0 and 59, multiple values can be separated with a comma. Typically, values are specified as top of the hour (0), or in multiples of 5 minute increments after the hour, for example, 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50 or 55.
<MINIMUM_UPDATES>	Minimum number of updates in the base table before a scheduled index updates is run.

The following example shows a Windows script:

```
clpplus -nw @sql-wrapper CustomIndexing_Step2_IndexCreate.sql
CustomIndexing_Step2_IndexCreate.log server1 50000 opx opuser
"password" "*" "*" "0,5,10,15,20,25,30,35,40,45,50,55" 1
```

The following example shows the same script on Linux:

```
clpplus -nw @sql-wrapper CustomIndexing_Step2_IndexCreate.sql
CustomIndexing_Step2_IndexCreate.log server1 50000 opx opuser
'password' "*" "*" "0,5,10,15,20,25,30,35,40,45,50,55" 1
```

These examples create an index with updates that start every 5 minutes of every hour of every weekday if there is a minimum of one update to the PROPERTYVALS_CLOB table.

Results

An index is created for long string fields.

Change the scheduled job that synchronizes the long string index in the database (Db2)

You can change the scheduled job that synchronizes the long string index. Scripts are provided for Windows and Linux.

When you install IBM OpenPages with Watson with Db2, you set up Db2 Text Search and create a job to synchronize the indexes. Do this task to refresh the indexes and the scheduled job.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to CLPPlus that can connect to the IBM OpenPages with Watson database server.

Note: For SQL tool information, see [“Database tool information”](#) on page xxxi.

2. Copy the CustomIndexing_Step3_IndexRefresh.sql script and the SQL files that the script invokes to the database server.

The files are in the <OP_HOME>/aura/bin directory.

3. Open a command or shell window, and navigate to the directory where you copied the files.

4. Run the following script:

```
clppplus -nw @sql-wrapper CustomIndexing_Step3_IndexRefresh.sql <LOG_FILE_NAME>
<DB2_SERVER_NAME> <DB2_PORT_NUMBER> <DATABASE_NAME> <OP_DB_USER> <OP_DB_PASSWORD>
<UPDATE_FREQUENCY_WEEKDAY> <UPDATE_FREQUENCY_HOUR> <UPDATE_FREQUENCY_MINUTE>
<MINIMUM_UPDATES>
```

Table 217. Refresh Db2 index required script parameters	
Required Parameter	Description
<LOG_FILE_NAME>	Name of the log file.
<DB2_SERVER_NAME>	Name of the Db2 server.
<DB2_PORT_NUMBER>	Port number of the Db2 database service
<DATABASE_NAME>	OpenPages database name.
<OP_DB_USER>	OpenPages user name for accessing the OpenPages database.
<OP_DB_PASSWORD>	OpenPages password for accessing the OpenPages database. If the password contains special characters, surround the password in quotation marks: - Windows: "password" - Linux: 'password'
<UPDATE_FREQUENCY_WEEKDAY>	Weekday update frequency. Accepted values are 0 - 6; multiple values can be separated with a comma. For all weekdays, use * (asterisk).
<UPDATE_FREQUENCY_HOUR>	Hourly update frequency. Accepted values are 0 - 23; multiple values can be separated with a comma. For all hours, use * (asterisk).
<UPDATE_FREQUENCY_MINUTE>	Minute update frequency. Accepted values are 0 - 59, multiple values can be separated with a comma. Typically, values are specified as top of the hour (0), or in multiples of 5-minute increments after the hour, for example, 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50 or 55.
<MINIMUM_UPDATES>	Minimum number of updates in the base table before a scheduled index updates is run.

The following example shows a Windows script:

```
clppplus -nw @sql-wrapper CustomIndexing_Step3_IndexRefresh.sql
CustomIndexing_Step3_IndexRefresh.log server1 50000 opx OPENPAGE "password"
"*" "*" "0,5,10,15,20,25,30,35,40,45,50,55" 1
```

The following example shows the same script on Linux:

```
clppplus -nw @sql-wrapper CustomIndexing_Step3_IndexRefresh.sql  
CustomIndexing_Step3_IndexRefresh.log server1 50000 opx OPENPAGE 'password' '*' '*'  
"0,5,10,15,20,25,30,35,40,45,50,55" 1
```

These examples schedule index synchronization to start every 5 minutes of every hour of every weekday if there is a minimum of one update to the PROPERTYVALS_CLOB table.

Results

Index synchronization jobs run at the interval specified.

Note: Changes to long string fields are not available for filtering until the next scheduled index job runs.

Drop a long string index

Remove the long string index. An index must be dropped before it can be re-created. Scripts are provided for Windows and Linux.

For more information about working with long string indexes, see [Text search index maintenance](#).

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to CLPPlus that can connect to the IBM OpenPages with Watson database server.

Note: For SQL tool information, see “[Database tool information](#)” on page xxxi.

2. Open a command or shell window, and navigate to the text-indexing directory as follows:

Windows

```
<OP_HOME>\aurora\bin\full-text-index
```

Linux

```
<OP_HOME>/aurora/bin/full-text-index
```

Note: If the database server is not on the same machine as the IBM OpenPages application server, you must copy the script and the SQL files that the script invokes to the database server.

3. Run the following SQL script:

```
clppplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql <LOG_FILE_NAME>  
<DB2_SERVER_NAME> <DB2_PORT_NUMBER> <DATABASE_NAME> <OP_DB_USER>  
<OP_DB_PASSWORD> <FORCE_DROP_INDEX>
```

Table 218. Enable Db2 drop index required script parameters	
Parameter	Description
<LOG_FILE_NAME>	Name of the log file.
<DB2_SERVER_NAME>	Name of the Db2 server.
<DB2_PORT_NUMBER>	Port number of the Db2 database service
<DATABASE_NAME>	Name of the OpenPages database instance.
<OP_DB_USER>	OpenPages user name for accessing the OpenPages database.

Table 218. Enable Db2 drop index required script parameters (continued)	
Parameter	Description
<OP_DB_PASSWORD>	OpenPages password for accessing the OpenPages database. If the password contains special characters, surround the password in quotation marks: • Windows: "password" • Linux: 'password'
<FORCE_DROP_INDEX>	Drops the index without regard to the status of any associated scheduled task. Values are Y (for Yes) or N (for No)

For example:

- Windows:

```
clpplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql
CustomIndexing_Step5_IndexDrop.log localhost 50000 OPX OPENPAGE
"password" Y
```

- Linux:

```
clpplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql
CustomIndexing_Step5_IndexDrop.log localhost 50000 OPX OPENPAGE
'password' Y
```

Results

You must re-create the index before you filter on the content of long string fields again. For details on creating a long string index, see [“Create a long string index for an Oracle database” on page 747](#).

Entity Move/Rename utility

The IBM OpenPages with Watson Entity Move/Rename utility allows batch processing of multiple Business Entities for overnight or weekend execution without running the risk of operations that time out. You can run the utility interactively or as a scheduled job.

Using the Entity Move/Rename utility, you can do the following:

- Rename a Business Entity hierarchy
- Simultaneously rename and move a Business Entity hierarchy

A single batch job can contain multiple independent operations, multiple dependent operations, or any combination thereof.

Each operation provides transactional consistency. If an operation fails, all the pending changes for this operation are rolled back. If an operation succeeds, all the changes are persisted.

Each rename, move, or combined operation runs in its own transactional context. So, failure in one operation does not result in the failure of the entire batch job.



CAUTION: Before running the utility, you must stop all application services to avoid data or security errors.

Entity Move/Rename utility prerequisites

Before you use the IBM OpenPages with Watson Entity Move/Rename utility, consider these prerequisites.

- A physical computer or VM that meets the OpenPages with Watson installation requirements. For detailed specifications, see the *IBM OpenPages with Watson Installation and Deployment Guide*.
- An application that produces either CSV (comma-separated value) files or Unicode tab delimited files. This application can be installed on any computer in your environment and is used to prepare the input data for the utility.
- User name and password for the Oracle or IBM Db2 account that owns the OpenPages application database schema (for example, OPENPAGES).

Configuring the Entity Move/Rename utility for a Db2 database

You must configure parameters in the OpenPages with Watson Entity Move/Rename utility before you use it in an IBM Db2 database environment.

Procedure

1. Go to the Entity Move/Rename utility installation location as follows:

`OP_Home|aurora|bin|batch_entity_move_rename_relative`

2. Open the `batch-entity-move-rename.ini` configuration file for editing.
3. Specify appropriate values for the following parameters for a Db2 database environment:

Table 219. Parameters for a Db2 database in the <code>batch-entity-move-rename.ini</code> file:	
Parameter Name	Description
<code>server_name</code>	Db2 database server.
<code>port_number</code>	Db2 service port number.
<code>db_Name</code>	OpenPages database name on Db2.
<code>user_name</code>	OpenPages database user name.
<code>password</code>	OpenPages database user password.
<code>data_format</code>	Format of the input file to the utility. Example: <code>csv</code> or <code>unicode-text</code> .
<code>input_file</code>	Name of the input file (including extension). Example: <code>'Sample-batch-entity-move-rename.txt'</code>
<code>code_page</code>	Code page that is used in the Db2 database. If the data_format parameter is set to the following value: • <code>csv</code> saved from Microsoft Excel, it is encoded in ANSI, then the code page must be set to 1252. • <code>unicode-text</code> and encoded in UTF-8 without BOM, then the code page must be set to 1208.

Table 219. Parameters for a Db2 database in the `batch-entity-move-rename.ini` file:
(continued)

Parameter Name	Description
skip_rows	The number of rows in the input files to skip on load. Example If the first row of the file: - Contains a list of column names, set the value to '1'. - Does not contain a list of column names, set this value to '0'.

4. Save and close the `batch-entity-move-rename.ini` configuration file.

5. Prepare the input file. See [“Prepare the input file for the Entity Move/Rename utility”](#) on page 710.

Prepare the input file for the Entity Move/Rename utility

The input file for the Entity Move/Rename utility can be in CSV or Unicode tab delimited format. You can use any editor to create the input files. Included in the utility installation folder is a sample Unicode text file (.txt format).

Important: On Linux, the text input file must be saved or converted to be encoded in UCS-2 Little Endian and have Linux end of line (LF) characters.

Tip: If you are using Microsoft Excel, you must save the spreadsheet as a CSV or tab delimited file.

The input file must have the following five columns of data:

Table 220. Columns in the input file		
Column Name	Description	Sample Value
Source entity location	The entity on which the operation is run.	/The Bank/USA/North East/Providence
Target entity location	The new parent entity for "move" and "move and rename" operations only. Note: - For Oracle "rename" operations only (no move), the value must be "-" (dash). - For Db2 "rename" operations only (no move), the value must be blank.	For "move" and "move and rename" operations: /Worldwide/ Americas/USA/NE
Run as user	Application user name, whose identity is used to run the operation.	OpenPagesAdministrator
New entity name	The new name after the operation for "rename" and "move and rename" operations only. Note: - For Oracle "move" operations only (no rename), the value must be "-" (dash). - For Db2 "move" operations only (no rename), the value must be blank.	For "rename" and "move and rename" operations: Boston

Table 220. Columns in the input file (continued)

Column Name	Description	Sample Value
Execution order	Establishes the operation execution order as follows: - Operations that specify the execution order are run before operations that do not. - Operations that have a numeric value in the execution order column are run in regular ascending ordering. If set, the value must to be a valid number; Otherwise, leave the field blank.	1

The following is a short description of the data in the sample .txt file that is included in the utility directory.

- The first line illustrates moving entity /The Bank/USA/North East/Providence to new location /Worldwide/Americas/USA/NE. Operation is to be run as the user SOXAdministrator. This operation is run first in the batch.
- The second line illustrates in place rename of the entity /Worldwide/Americas/USA/NE/ Providence. Entity name changes to Boston. Target location does not apply and is set to "-". This entry has a dependency on the previous move operation and has higher number in the execution order column. Also, it references to the new entity location that will be in effect after the first operation completes.
- If the first operation fails for any reason, this operation fails as well and the entity location would be incorrect.
- The third line illustrates simultaneous move of the entity /The Bank/USA/Midwest/Chicago to new location /Worldwide/Americas/USA/MW and rename to Detroit. This operation has no dependencies and will be run after the first two complete.

If you have an Oracle database with the 32-bit SQL*Loader utility in a Linux environment, see the topic: [“Avoid error 0509-036 when you use the 32-bit Oracle SQL*Loader” on page 761](#). Otherwise, run the IBM OpenPages with Watson Entity Move/Rename utility.

Running the Entity Move/Rename utility interactively for a Db2 database

Use the following steps to run the IBM OpenPages with Watson Move/Rename utility interactively in an IBM Db2 database environment.

Before you begin, make sure that you prepared the input file. See [“Prepare the input file for the Entity Move/Rename utility” on page 710](#) for instructions.

Procedure

1. Move the input file into the utility installation directory, which is at:

```
OP_Home|aurora|bin|batch_entity_move_rename_relative
```

2. Validate that the **input_file** parameter in the batch-entity-move-rename.ini configuration file is correctly set to the input file name. For more information, see [“Configuring the Entity Move/Rename utility for a Db2 database” on page 709](#).
3. For Windows operating systems only: Start the Db2 command line processor first by opening a command window and entering the **db2cmd** command.
4. From the location where the utility is installed, run the batch command file and review the output on the screen.

Windows

batch-entity-move-rename.cmd

Linux

batch-entity-move-rename.sh

5. Upon completion, review the following log files for any errors:

- batch-entity-move-rename-load.log
- batch-entity-move-rename-proc.log

If any errors are reported and you are unable to fix them, contact IBM OpenPages Support. Make sure you supply a copy of the screen that contains the error messages and all the log files that are generated by the tool.

Running the Entity Move/Rename utility as a scheduled task

You can set up a scheduled task to run the IBM OpenPages with Watson Entity Move/Rename utility.

Depending on your environment, you can run the batch-entity-move-rename batch command file by using any scheduling application. For example, in Windows, you might use the built-in Windows scheduler. In Linux, you might set up a **cron** job.

Important: If you are using a Db2 database in a Windows environment, you must run the batch command file within the **Db2 Command Line Processor**.

If the job fails, the batch command returns a non-zero exit code. You can redirect the console output to a log file. For example, in Windows:

```
batch-entity-move-rename.cmd >> batch-entity-move-rename.log
```

The following files are overwritten on each run:

- batch-entity-move-rename-load.log
- batch-entity-move-rename-proc.log

These files can be saved, either manually or through a script, if log archives are needed.

Impact of the Entity Move/Rename utility on the OpenPages application

The Entity Move/Rename utility works directly against the IBM OpenPages with Watson database repository. As a result, the Java based OpenPages application is unaware of the changes made to the entity hierarchy and folder structure.

As a result, internal application caches might become out of sync with the data in the repository and lead to discrepancies in the application user interface.

It is required that after you run the tool you restart application services, or run the tool when application services are stopped.

Also, ensure that the **OPBackup** command is not running during execution, and that all batch rename and move operations are completed before you run a backup.

Chapter 22. Using IBM OpenPages with Watson utilities with Oracle databases

You can use these utilities with your Oracle database for backing up and restoring OpenPages with Watson and Cognos files and databases, and setting up a test environment.

Oracle databases and the backup and restore utilities

The backup and restore utilities are installed during the IBM OpenPages with Watson installation.

Use these utilities to back up and restore the OpenPages with Watson environment:

- OpenPages with Watson backup (OPBackup) and restore (OPRestore) are used to backup and restore the OpenPages with Watson application and database
- Cognos backup (OPCCBackup) and restore (OPCCRestore) are used to backup and restore OpenPages with Watson Cognos files and the content store.
- Users can choose to execute a live OPBackup. When running live OPBackup, OpenPages with Watson services are not restarted on the application server, allowing for maximum uptime of the application. By default, the services will be restarted.

Prerequisite: Oracle client software

To use the backup and restore utilities that are included with IBM OpenPages with Watson, the Oracle client software must be installed on both the OpenPages with Watson application server and OpenPages with Watson Cognos server machines.

Note: For the currently supported versions of the Oracle client software, see the [Supported Environments website](#) or the *IBM OpenPages with Watson Installation and Deployment Guide*.

Oracle Data Pump

Oracle Data Pump provides a server-side infrastructure for very high-speed loading and unloading of data and metadata to and from the database.

Oracle Data Pump is used by the IBM OpenPages with Watson application and Cognos backup and restore utilities and was automatically configured during the OpenPages with Watson installation or upgrade process. If necessary, you can modify Oracle Data Pump settings.

Important:

- The Oracle Data Pump utility creates database backups on the database server. To ensure the database backups are available in the event of a server failure, make sure to copy these backup (dump) files to a different server or external device (such as a tape drive) after the OPBackup or OPCCBackup tool has completed.
- Before you use the Cognos backup utility for the first time, you must configure the Oracle Data Pump datapump directory. You do this by running an SQL script. For details, see [“Configuring or updating the Oracle Data Pump directory” on page 725](#).

If you change the name or location of the datapump directory, you can also use this script to update the configuration information.

- Oracle Data Pump commands IMPDP and EXPDP should be used because the IMP and EXP commands are not supported.

Email notification for backup jobs

You can configure email notification when you complete an IBM OpenPages with Watson application backup or Cognos backup job.

Note:

- Log files for email notification are stored in the logs folder in the following locations. A timestamp is included in the log file names.

- For OPBackup (OpenPages with Watson application backup):

```
<OP_Home>|aurora|bin|logs
```

- For OPCCBackup (Cognos backup):

```
<CC_Home>|tools|bin|logs
```

- Make sure to set rules in your email client to never send emails from the OpenPages with Watson application server to the Spam or Junk mail folders.

Configuring backup job notification

Use this procedure to configure email parameters for IBM OpenPages with Watson and Cognos backup jobs.

Procedure

- Open a command or shell window and do one of the following.
 - For an OPBackup (OpenPages with Watson application backup), navigate to the `op-backup-restore.env` file in the `<OP_HOME>/aurora/bin` directory.
 - For a OPCCBackup (Cognos backup), navigate to the `op-cc-backup-restore.env` file in the `bin` directory where `<cc_home>` represents the installation of Cognos.
 - For Microsoft Windows, the back up path is `OPBackup <path-to-back-up-location>`
 - For Linux, the back up path is `OpBackup.sh <path-to-back-up-location>`where `<path-to-backup-location>` is the full path of the directory where the backed up files are located on the application server. If a file path is not specified, the OPBackup command uses, by default, the backup location specified in the `BACKUP_LOCATION` parameter of the `<OP_Home>|aurora|bin|op-backup-restore.env` file.
- Open the selected `.env` file in a text editor.
- Specify a value after the equal sign (=) for the parameters described in the following table and save the `.env` file.

Table 221. Backup email parameters	
Parameter name	Description
BACKUP_EMAIL_NOTIFICATION_SERVER=	The host name of the outgoing mail server.

Table 221. Backup email parameters (continued)	
Parameter name	Description
BACKUP_EMAIL_NOTIFICATION_TO_EMAIL_ID=	The name of recipients that will receive the email notification. Separate email addresses with a comma (,). Note: Do not type a comma after the last email address. Example emailid1@yourdomain.com,emailid2@yourdomain.com
BACKUP_EMAIL_NOTIFICATION_FROM_EMAIL_ID=	The name that will appear as the sender of the notification email in the From: field of the email. The email address is also used as the personal name.
BACKUP_EMAIL_NOTIFICATION_SUCCESS_MSG_FILE=BACKUP_SUCCESS_MSG.txt	The BACKUP_SUCCESS_MSG.txt file is the default file containing the message text that will be used if the OPBackup.cmd completes successfully. You can modify the message text in the BACKUP_SUCCESS_MSG.txt file. The first line of the file is used as the email's subject.
BACKUP_EMAIL_NOTIFICATION_FAIL_MSG_FILE=BACKUP_FAIL_MSG.txt	The BACKUP_FAIL_MSG.txt file is the default file that contains the message text that is used if the OPBackup.cmd fails with errors. You can modify the message text in the BACKUP_FAIL_MSG.txt file as wanted. The first line of the file is used as the email's subject.

Asynchronous background jobs and administrative functions

IBM OpenPages with Watson supports asynchronous execution of processes in the background.

The most common examples of these type jobs are FastMap web-based data import jobs, object resets, and reporting schema generation.

For example, after a user submits a data import file, that file is queued for loading and the import process occurs in the background. Because it is important for asynchronous background jobs to run to completion, certain administrative operations are suspended until all background jobs complete.

By default, the following administrative functions will not start until background jobs are complete:

- OPBackup command
- OPRestore command
- System Administrative Mode (SAM)

Note: To disable the default setting that checks for background jobs before you start **OPBackup** or **OPRestore**, see [“Enabling and disabling asynchronous background processes checking”](#) on page 682.

If asynchronous processes are found, error messages are written to the OPBACKUP restore log.

Example

The following is a sample error log message that occurred when an OPBackup command was initiated while the reporting schema was still being generated.

Note: The .log file name has the format `op_backup_<yyyy_mm_dd_hh_mm_ss>.log`

Where:

`<yyyy_mm_dd_hh_mm_ss>` represents the year_month_day_hour_minute_second. For example:

Windows

`C:\OpenPages\openpages-backup-restore\op_backup_2019_07_26_09_35_42.log`

Linux

`/opt/OpenPages/openpages-backup-restore/op_backup_2019_07_26_09_35_42.log`

Sample error log messages follow.

- For Oracle database environments, a sample error log message might look similar to this text:
 - can-proceed:
[exec] declare
[exec] *
[exec] ERROR at line 1:
[exec] ORA-20001: There are existing processes running.
[exec] Please let them finish or terminate them before proceeding.
[exec] ORA-06512: at line 7
[exec]
 - can-proceed:
[exec] declare
[exec] *
[exec] ERROR at line 1:
[exec] ORA-20001: There are existing object reset operations running.
[exec] Please let them finish or terminate them before proceeding.
[exec] ORA-06512: at line 7
[exec]
- For IBM Db2 environments, a sample error log message might look similar to this text:
 - can-proceed:
[exec] ERROR near line 26:
[exec] SQL0438N Application raised error or warning with diagnostic
[exec] text: "There are existing processes running. Please let them
[exec] finish or termi".
 - can-proceed:
[exec] ERROR near line 26:
[exec] SQL0438N Application raised error or warning with diagnostic
[exec] text: "There are existing object reset operations running.
[exec] Please let them finish or termi".

Enabling and disabling asynchronous background processes checking

By default, IBM OpenPages with Watson does not allow a backup (OPBackup) or restore (OPRestore) operation to start until all asynchronous background jobs are complete.

It is best to run all jobs to completion before you start a backup or restore operation. However, this check can be enabled or disabled as follows.

Procedure

1. Open a command or shell window on the OpenPages with Watson server.
2. Navigate to the `op-backup-restore.env` file in the `<OP_Home>/aurora/bin` directory.
3. Open the `op-backup-restore.env` file in a text editor.
4. Set the `CHECK_BACKGROUND_PROCESSES` parameter in the file to true or false.
Setting the value to true enables the asynchronous background job. If background processes are running, this value prevents OPBackup or OPRestore from starting. True is the default value. false disables the validation check for asynchronous background jobs. OPBackup or OPRestore start even if background processes are running.

Encrypting database passwords in the backup-restore utility environment files

Passwords that are used by the IBM OpenPages with Watson, and Cognos database user accounts within the backup-restore environment files are encrypted, by default, during installation.

If you change the value of the password parameters within the following environment files, the value is in plain text until it is encrypted.

- `op-backup-restore.env` database password parameters (the file is stored on the application server):
 - `DB_SYSTEM_PWD=`
 - `DB_SYS_PWD=`
 - `DB_OP_PWD=`
- `op-cc-backup-restore.env` database password parameters (the file is stored on the reporting server):
 - `DB_CC_PWD=`

For security purposes, encrypt the changed passwords by completing the following procedure.

Important: In a horizontal clustered environment, you must complete this procedure on each application server or reporting server in the horizontal cluster.

Procedure

1. Open a command or shell window on the OpenPages with Watson server.
2. Go to the `<OP_HOME>/aurora/bin` directory.
3. To encrypt changed database password parameters in the `op-backup-restore.env` environment file, run the following command:
 - On Windows operating systems: `OPBackup.cmd secure`
 - On Linux operating systems: `./OPBackup.sh secure`
4. To encrypt changed database password parameters in the `op-cc-backup-restore.env` environment file, do the following steps:
 - a) Open a command or shell window on the reporting server.
 - b) Go to the `<CC_Home>/tools/bin` directory.
`<CC_Home>` is the installation location of Cognos.
 - For Microsoft Windows, `<CC_Home>` is `C:\OpenPages\CommandCenter`.
 - For Linux, `<CC_Home>` is `opt/OpenPages/CommandCenter`.
 - c) Type the following backup command:
 - On Windows: `OPCCBackup.cmd secure`
 - On Linux: `./OPCCBackup.sh secure`

The OPBackup utility

OPBackup is the IBM OpenPages with Watson backup utility that backs up the necessary product files and database content on the server where it is run. The OPBackup utility creates a backup file that can be used by the OpenPages restore utility (OPRestore).

When you use the OPBackup utility, the following OpenPages with Watson resources are backed up:

- The OpenPages with Watson application
- The OpenPages with Watson storage folder and its content
- The OpenPages with Watson application environment files

In a horizontal clustered environment, if you run OPBackup on a non-administrative server, the application database is not included in the backup. To include this database in a backup file, run OPBackup on an administrative server.

OPBackup does not back up standard tools by default. If you want to include additional files or directories, you must add them to a manifest file before you run the backup. For more information, see [“Backing up custom files” on page 683](#).

Depending on your configuration, if any asynchronous background jobs are detected, an OPBackup job will exit and possibly display errors (see [“Asynchronous background jobs and administrative functions” on page 681](#)).

You can also configure email notification upon completion of an OPBackup. For details, see [“Email notification for backup jobs” on page 679](#).



Attention: If you have global search enabled, global search must be disabled before running the OPBackup and OPRestore utilities. For more information, see [“Using OPBackup and OPRestore when global search is enabled” on page 653](#).

Modifying the backup-restore environment file

The IBM OpenPages with Watson storage location is set during the installation process. Use the following scenarios to determine if you need to modify the OPSTORAGE_LOCATION parameter in the `op-backup-restore.env` file.

By default, the `op-backup-restore.env` file is located in the `bin` directory as follows: `<OP_Home>|aurora|bin`.

- For Microsoft Windows: `<OP_Home>` is `C:\OpenPages`.
- For Linux: `<OP_Home>` is `/opt/OpenPages`.

Scenario 1: The root installation path of the OpenPages with Watson storage location changed after installation

If you modify the root path of the IBM OpenPages with Watson storage location in the `storageservers` table after installation, make sure you update the OPSTORAGE_LOCATION parameter in the `<OP_Home>|aurora|bin|op-backup-restore.env` file to match the new root path (OpenPages with Watson storage location).

If these locations do not match, the OPBackup utility will capture incorrect or stale storage folders.

Scenario 2: The OPBackup utility is running on a non-administrative server

If you are running the OPBackup utility on a non-administrative server, you must update the OPSTORAGE_LOCATION parameter in the `<OP_Home>|aurora|bin|op-backup-restore.env` file on the non-administrative server to point to the remote location of the `openpages_storage` folder on the administrative server.

Make sure to use forward slashes as the path separator in this UNC path.

Example

```
//<host_server>/openpages_storage
```

Where:

<host_server> is the name of the administrative server.

Backing up custom files

You can include custom files, such as custom JSPs or other files that are specific to your environment, in backups by using a manifest file. A manifest file is a text file that contains the full path name to any directory or file that needs to be included in the backup.

For example, if you want to back up `openpages-ext.jar`, add its full path to the manifest file:

```
/opt/opuser/IBM/OpenPages/aurora/lib/openpages-ext.jar
```

Before you begin

- You must list all of your custom directories and files in a manifest. If you have any questions about the location of your custom data, contact IBM OpenPages Support.
- In a horizontal clustered environment, you must perform this procedure on each application server in the horizontal cluster.

Procedure

1. Log on to the application server.
2. If you have custom JSPs, do the following steps:
 - a) Create a zip file called `solutions-sosa-files.zip` that contains your custom JSPs and related files.

Tip: You can use a different name, but it must follow the convention `*-sosa-files.zip`. Also, you must add it to the `<OP_HOME>/aurora/bin/op-backup.manifest` file. Only `solutions-sosa-files.zip` is backed up and restored by default.
 - b) Put the `solutions-sosa-files.zip` file in the `<OP_HOME>/applications` directory.
 - When you run `OPBackup`, the zip file is included in the backup.
 - When you run `OPRestore`, the zip file is restored to `<OP_HOME>/applications` and is also extracted to `<OP_HOME>/wlp-user/shared/apps/op-apps.ear/sosa.war/`
3. Open the `<OP_HOME>/aurora/bin/op-backup.manifest` file in a text editor.
4. Add custom files or directories, other than JSPs, to the `op_backup.manifest` file.

You can specify directories or individual files. For each file or directory, create a new line and type its full path..
5. Save the manifest file using the current location and name.

Running the OPBackup command

When you use the IBM OpenPages with Watson application backup utility, run the `OPBackup` command in a command or shell window.

The `OPBackup` command does the following:

- Stops all OpenPages with Watson services before performing any backup operation
- Backs up OpenPages with Watson application and environment files
- Restarts the services when the backup activities are complete

See [“Running a live OpenPages with Watson backup” on page 684](#) if you want to perform a backup without stopping services.

Procedure

1. If global search is enabled, disable it:
 - a) Log in to OpenPages as an administrator.
 - b) Click **Administration > Global Search > Disable**.
2. Open a command or shell window on the OpenPages with Watson admin application server.
3. Navigate to the `<OP_Home>/aurora/bin` directory.
4. Run the following backup command:

Windows

```
OPBackup <path-to-backup-location>
```

Linux

```
./OPBackup.sh <path-to-backup-location>
```

Where `<path-to-backup-location>` is the full path of the directory where the backed up files are located on the OpenPages with Watson application server. If a file path is not specified, the OPBackup command uses, by default, the backup location specified in the `BACKUP_LOCATION` parameter of the `<OP_Home>/aurora/bin/op-backup-restore.env` file.

You can use the following optional parameters:

- `app-nodb`: Back up everything except the OpenPages database.
- `dbonly`: Back up only the OpenPages database. (Applies to Oracle databases only. To back up an IBM Db2 database, use the utilities that are provided with Db2.)

For example:

```
./OPBackup.sh <path-to-backup-location> app-nodb
```

Backing up the OpenPages database (Oracle)

You can use the OPBackup utility to back up the IBM OpenPages with Watson databases.

About this task

Note: You can back up the databases by using other methods. Some examples of alternative methods include:

- Doing a full physical backup by using RMAN
- Doing a combination of full and incremental backup by using RMAN
- Doing an Oracle data pump export.

If you want to use an alternative method, it is critical that you have the necessary skills available within your organization to complete all aspects of the backup and restore activity.

Procedure

1. Make sure that no OpenPages with Watson processes are running, such as object reset jobs.
2. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see [Chapter 24, “Starting and stopping servers,” on page 841](#).
3. Open a command or shell window on the admin application server.
4. Go to the `<OP_HOME>/aurora/bin` directory.
5. Do a full database backup of the OpenPages schema by using OPBackup.

Windows:

```
OPBackup.cmd <backup_directory> dbonly
```

Linux:

```
./OPBackup.sh <backup_directory> dbonly
```

The *<backup_directory>* is the full path to a directory on the database server. This directory is where the log files are saved. If the file path is not specified, the OPBackup command uses the location that is specified by the **BACKUP_LOCATION** parameter in the *<OP_HOME>/aurora/bin/op-backup-restore.env* file.

A dump file is created in the OP_DATAPUMP_DIRECTORY directory.

6. Examine the backup log and make note of the dump file name. The naming convention is *openpage_<timestamp>.dmp*.

Running a live OpenPages with Watson backup

A live IBM OpenPages with Watson backup means that the application can continue running while the backup is in progress. The services are not stopped during the backup.

Note: Run live OpenPages with Watson backups during off-peak hours because the backup consumes processing resources.

You might encounter errors such as the following during the database export portion of the live OP backup:

```
[exec] ORA-31693: Table data object "OPENPAGES"."table_name"  
failed to load/unload and is being skipped due to error:  
[exec] ORA-02354: error in exporting/importing data  
[exec] ORA-01555: snapshot too old: rollback segment number #  
with name "rollback_segment_name" too small
```

This might happen if there is a relatively high level of data modification transactional activity on the system during the backup. Run live OP backup when transactional activity is low. If this is not possible or not desirable, or if the error keeps happening, it may be possible to avoid this error by setting UNDO_RETENTION initialization parameter to a higher (possibly much higher) value, at least for the duration of the backup. Setting UNDO_RETENTION to a higher value, may result in a growth of UNDO table space, so it should be done by an experienced database administrator or with the assistance of IBM OpenPages Support.

To use the OpenPages with Watson application backup utility live, you run the OPBackup command with the nosrvrst option. This does the following:

- Backs up OpenPages with Watson application and environment files
- Exports the OpenPages with Watson application database

Procedure

1. Open a command or shell window on the OpenPages with Watson admin application server.
2. Navigate to the *<OP_Home>/aurora/bin* directory.
3. Type the following backup command:

Windows

```
OPBackup <path-to-backup-location> nosrvrst
```

Linux

```
OPBackup.sh <path-to-backup-location> nosrvrst
```

where:

Windows

<path-to-backup-location> is <oracle_base>\admin\<SID>\dpdump

Linux

<path-to-backup-location> is <oracle_base>/admin/<SID>/dpdump

OpenPages with Watson backed-up content

The backup process creates a ZIP file (.zip) in the <backup-directory-name> directory.

The ZIP file contains the following necessary backed up databases and data files:

- OpenPages application database
- OpenPages properties files (such as `aurora.properties` and `Server<#>-sosa.properties`).
- Application server configuration files for IBM WebSphere.
- The `openpages-storage` directory.
- Pointers to the database schema dump extracts.
- Files and directories that are listed in the manifest file (such as `solutions-sosa-files.zip`).

The manifest file is `<OP_HOME>/aurora/bin/op-backup.manifest`

Note:

- If a backup file is 4 GB or larger, configure the OPBackup utility to use gzip (GNU zip). Gzip produces an archive with an extension of `.tar.gz`. To view and extract the contents of the archive file, use WinZip 12 (or higher) or WinRAR 3.71 (or higher).
- The OPBackup utility adds a timestamp on the .zip and log files it creates.

The ZIP file can be used as a parameter to the OPRestore command to restore the installation-specific OpenPages with Watson files and the database. Each time the OPBackup command is run, a separate ZIP file is created and each data file is identified by a unique name.

The OPBackup log file

The backup process creates a log file, which is identified by a unique name in the <backup-directory-name> folder. Each time you run the OPBackup command, a separate log file is generated.

Configuring OPBackup to use GZIP

If a ZIP backup file grows beyond the 4-GB limit of ZIP file capacity, you can configure the OPBackup utility to use gzip (GNU zip). After the file is configured, new backup files will have a `.tar.gz` extension. The OPRestore utility detects if a file is in ZIP or gzip format and processes the file accordingly.

Procedure

1. From a command or shell window, navigate to the `op-backup-restore.env` file in the `bin` directory as follows.
 - For Windows, the installation directory is `c:\<OP_Home>\aurora\bin`
 - For Linux, the installation directory is `<OP_Home>/aurora/bin`
2. Open the `op-backup-restore.env` file in a text editor of your choice.
3. Change the `USE_GZIP_COMPRESSION=` setting from `false` to `true`.

Enabling and disabling storage backup

By default, the IBM OpenPages with Watson backup includes the storage folder and its content. You can disable storage backup by setting the `BACKUP_OP_STORAGE` parameter in the `op-backup-restore.env` file.

Procedure

1. Open a command or shell window on the OpenPages with Watson server.
2. Navigate to the `op-backup-restore.env` file in the `bin` directory as follows.

Table 222. Installation locations	
Operating system	Installation location
Windows	<OP_HOME>\aurora\bin
Linux	<OP_HOME>/aurora/bin

3. Open the `op-backup-restore.env` file in a text editor of your choice.
4. Set the value of the `BACKUP_OP_STORAGE` parameter in the file to one of the following:

Table 223. BACKUP_OP_STORAGE parameter values and their meanings	
If the value is set to...	Then...
true	The storage folder and its content are backed up. This is the default value.
false	The storage folder and its content are not backed up.

5. When finished, save the changes to the file and exit the editor.

The OpenPages restore utility on the Oracle database

OPRestore is the IBM OpenPages with Watson restore utility that restores the OpenPages files and database content on the server from which it was originally run. The OPRestore utility uses a backup file created by the OpenPages with Watson backup utility (OPBackup).

Important: To refresh a "test" environment, see [“Refreshing a test environment from backup files”](#) on page 736.

As part of the restoration process, the following OpenPages with Watson resources are restored:

- The OpenPages with Watson application
- The OpenPages with Watson storage folder and its content
- The OpenPages with Watson application environment files

Important: In a horizontal environment, if OpenPages with Watson backup is run on a non-administrative server, the application database is not included in the backup, so will not be restored.

Depending on your configuration, an OPRestore job may not start until all asynchronous background jobs run to completion (see [“Asynchronous background jobs and administrative functions”](#) on page 681).

Running the OPRestore command

You can restore a backup using the OPRestore command.

Before you begin

If you used OPBackup, the zip file should contain the database dump files (`.dmp`). If the dump files are not in the zip file, copy them to the backup location before you start the restore.

Procedure

1. If you enabled the global search component during backup, recreate your search index so that your search results are synchronized.

- a) Click **Administration** > **Global Search**.
 - b) Click **Disable** to disable the global search component.
 - c) Click **Drop** to drop the search indexes.
 - d) Click **Create** to recreate the search indexes.
2. Stop the IBM Cognos service.
 3. From a command or shell window, navigate to the <OP_Home>/aurora/bin directory:
 4. Execute the following command:

Windows

```
OPRestore <backup-file-name> <path-to-backup-location>
```

Linux

```
./OPRestore.sh <backup-file-name> <path-to-backup-location>
```

Where <backup-file-name> is the name of the backup file (without the .zip or tar.gz file extension)

You can use the following optional parameters:

- app-nodb: Restore everything except the OpenPages database.
- dbonly: Restore only the OpenPages database. (Applies to Oracle databases only. To back up an IBM Db2 database, use the utilities that are provided with Db2.)

For example:

```
./OPRestore.sh <backup-file-name> <path-to-backup-location> app-nodb
```

What to do next

Preferences related to the long string text index won't be exported by “Running the OPBackup command” on page 719, and therefore are not restored. You must “Create a long string index for an Oracle database” on page 747 pointing to the database server you are restoring to.

OPRestore log files

The restore process creates a log file identified by a unique name in the <backup-directory-name> folder. Each time you run the OPRestore command, a separate log file is created.

Note: Oracle Data Pump log files for database imports are created on the database server.

Using the Cognos backup utility

OPCCBackup is the Cognos utility that backs up the necessary Cognos files. The OPCCBackup utility creates a backup file that can be used by the Cognos restore utility (OPCCRestore).

To back up or restore the IBM Db2 databases for IBM OpenPages with Watson, you must use the utilities that are provided with Db2. For more information about the databases in IBM OpenPages with Watson and backing up or restoring them, see “Db2 database backup and restore for OpenPages” on page 690.

When you use the OPCCBackup utility, the following Cognos resources are backed up.

- Cognos reports
- Branding and environment files

You can configure e-mail notification (with an attached log file) upon the completion of an OPCCBackup. For details, see “Email notification for backup jobs” on page 679.

Oracle Data Pump configuration on a first time use

Before you use the Cognos backup utility for the first time, you must configure Oracle Data Pump by running an SQL script.

This task is required.

For details on running the script, see [“Configuring or updating the Oracle Data Pump directory” on page 725](#).

The script configures a data pump storage directory for the user name specified in the <user_name> parameter. If a datapump storage directory was already configured for the specified user name, the script will display an appropriate message.

The OpenPages with Watson file storage directory

By default, OP_DATAPUMP_DIRECTORY is the name of the directory used for storing Cognos Content Store database backup files. The path to this directory on the database server varies and depends on how it was defined.

If the OP_DATAPUMP_DIRECTORY storage directory does not already exist on the database server, you must run the script to create the directory.

Configuring or updating the Oracle Data Pump directory

The script used in this procedure requires access to the content of the installation kit: OP_<version>_Main.

Use the following SQL*Plus script to:

- Create the Oracle Data Pump datapump directory for first time use of the CommandCenter backup utility.
- Update configuration information if you modified the log file name or datapump directory location to reflect changes in your environment.

Procedure

1. Log on to a machine with SQL*Plus and a connection to the CommandCenter database instance.
2. Open a command or shell window.
3. Go to the following directory:

```
/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/  
UPGRADE_SCRIPTS
```

4. Run the update-datapump-directory.sql script as follows and substitute values for each parameter:

```
sqlplus /nolog @sql-wrapper update-datapump-directory <log_file_name>  
<tns_name_alias> SYSTEM <password> <create|update> <directory_location>  
<user_name>
```

Note: All parameters are required.

Table 224. Parameters for Oracle Data Pump SQL script	
This parameter...	Represents...
<log_file_name>	The user-defined name of the log file that the script will create and write information to. Examples Linux: /tmp/update-datapump.log Windows C:\temp\update-datapump.log

Table 224. Parameters for Oracle Data Pump SQL script (continued)	
This parameter...	Represents...
<tns_name_alias>	The database Oracle TNS entry to be used by the OpenPages CommandCenter database instance on the reporting server computer.
<password>	The password for the Oracle SYSTEM user account. If the password contains special characters, surround the password in quotation marks: • Windows: "password" • Linux: 'password'
<create update>	Specify one of the following values: • create - use this if you are configuring Data Pump for first time use. • update - use this if you are modifying the <Directory Location> parameter.
<directory_location>	The full directory path on the database server where the backed up files will be placed.
<user_name>	The user name to be used with the Cognos account for the CommandCenter database schema (Content Store).

Example:

```
sqlplus /nolog @sql-wrapper update-datapump-directory.sql C:\temp\update-datapump.log
OP SYSTEM "password" create d:\cc_backup cognos
```

```
sqlplus /nolog @sql-wrapper update-datapump-directory.sql /tmp/log
op SYSTEM 'password' create TESTDIR openpage
```

Running the OPCCBackup command

When you use the Cognos backup utility, you run the OPCCBackup command in a command or shell window. The OPCCBackup command uses Oracle Data Pump to export the database (services can continue to run during the backup).

Note: Oracle Data Pump backup files are created on the database server.

Procedure

1. From a command or shell window, navigate to the <CC_Home>/tools/bin, where <CC_Home> represents the installation location of the Cognos application.
2. Run the following backup command:

Windows

```
OPCCBackup <path-to-backup-location>
```

Linux

```
OPCCBackup.sh <path-to-backup-location>
```

Where:

<path-to-backup-location> is the full path of the directory where the backed up files are located on the Cognos server. The file path is optional.

Note: If no file path is specified, the OPCCBackup command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the <CC_Home>\tools\bin\op-cc-backup-restore.env file.

The following table lists the default content store database export location specified in the environment file.

Where <SID> is the Oracle System Identifier (for example, OP).

The default content store database export locations are:

Windows: <oracle_base>\admin\<SID>\dpdump

Linux: <oracle_base>/admin/<SID>/dpdump

If you get the warning `tools.jar file is not found`, see the following [technote](#).

The OPCCBackup log file

The backup process creates a log file, which is identified by a unique name in the <backup-directory-name> folder. Each time you run the OPCCBackup command, a separate log file is generated.

Cognos backed-up content

The Cognos backup process creates a ZIP file (.zip) in the <backup-directory-name> directory. This ZIP file contains the necessary report and environment files that can be used by the Cognos restore utility (OPCCRestore).

Note:

- If a backup file is very large (4 GB or larger), configure the OPCCBackup utility to use gzip (GNU zip). Gzip produces an archive with an extension of .tar.gz. To view and extract the contents of the archive file, use WinZip 12 (or higher) or WinRAR 3.71 (or higher).
- The OPCCBackup utility adds a military timestamp on the .zip and log files it creates.

The ZIP file can be used as a parameter to the OPCCRestore command to restore the installation-specific IBM OpenPages with Watson files and the database. Each time the OPCCBackup command is run, a separate ZIP file is created and each data file is identified by a unique name.

Configuring OPCCBackup to use GZIP

If a ZIP backup file grows beyond the 4-GB limit of ZIP file capacity, you can configure the OPCCBackup utility to use gzip (GNU zip). Once the file is configured, new backup files will have a .tar.gz extension. The OPCCRestore utility will detect if a file is in ZIP or gzip format and process it accordingly.

Procedure

1. From a command or shell window, navigate to the op-cc-backup-restore.env file in the bin directory as follows, where <CC_Home> represents the installation location of the Cognos application
 - For Windows, the directory is: <CC_Home>\tools\bin. By default, <CC_Home> is C:\OpenPages\CommandCenter
 - For Linux, the directory is: <CC_Home>/tools/bin. By default, <CC_Home> is opt/OpenPages/CommandCenter
2. Open the op-cc-backup-restore.env file in a text editor.
3. Change the **USE_GZIP_COMPRESSION=** setting in the file from false to true:

Using the Cognos restore utility

OPCCRestore is the IBM OpenPages with Watson Cognos utility that restores the necessary Cognos files and Content Store on the server from which it was originally run. The OPCCRestore utility uses a backup file created by the OpenPages with Watson Cognos backup utility (OPCCBackup).

Note: To refresh a "test" environment, see [“Refreshing a test environment from backup files” on page 736](#).

As part of the restoration process, the following Cognos resources are restored:

- Cognos reports
- Content Store
- Branding and environment files

Running the OPCCRestore command

You can restore backed up Cognos data using the OPCCRestore utility as follows.

Procedure

1. Stop the IBM Cognos service on the administrative server and any non-administrative servers in the cluster. For details, see [“Starting and stopping the Cognos services” on page 849](#).
2. Stop the IBM Cognos Configuration tool, if it is running, on all cluster members.
3. From a command or shell window, navigate to the `<CC_Home>/tools/bin` directory where `<CC_Home>` represents the installation location of the Cognos application.
 - For Windows, the installation location is `C:\OpenPages\CommandCenter`.
 - For Linux, the installation location is `/opt/OpenPages/CommandCenter`
4. On the administrative Cognos server, run the following command:

Windows

```
OPCCRestore <backup-file-name> <path-to-backup-location>
```

Linux

```
OPCCRestore.sh <backup-file-name> <path-to-backup-location>
```

Where:

`<backup-file-name>` is the name of the backup file (without the `.zip` or `tar.gz` file extension).

Note: `<path-to-backup-location>` is the full path of the directory where the backed up files are located on the Cognos server. The file path is optional.

If no file path is specified, the OPCCRestore command uses, by default, the backup location specified in the `BACKUP_LOCATION` parameter of the `<CC_Home>/tools/bin/op-cc-backup-restore.env` file.

5. Start the IBM Cognos service on the administrative server and on any non-administrative servers in the cluster. For details, see [“Starting and stopping the Cognos services” on page 849](#).

The OPCCRestore log file

The restore process creates a log file identified by a unique name in the `<backup-directory-name>` folder.

Each time you run the OPCCRestore command, a separate log file is created.

Note: Oracle Data Pump log files for database imports are created on the database server.

Using Oracle online database backup (RMAN) for point-in-time recovery

To perform an online backup of the IBM OpenPages with Watson database, using custom OpenPages scripts that utilize Oracle's Recovery Manager (RMAN) facility.

Knowledge of basic Oracle database backup and recovery operations is necessary, as well as use of RMAN. For more information on the use of RMAN for online database backup and recovery, see the Oracle documentation.

Oracle online database backups

Unlike the IBM OpenPages with Watson OPBackup utility, the Oracle online database backup function does not require shutting down access to database operations before backing up the database.

It can perform an incremental backup in the background at a designated interval while allowing full user access to the OpenPages with Watson database and OpenPages with Watson services. It also allows "point in time" recovery of the OpenPages with Watson database with minimal chance of data loss.

In contrast, OPBackup and OPRestore can only do a full backup and restore of the database and other files (not incremental). Because full backups are typically performed less frequently than incremental backups, the possibility of significant data loss in the event of a system crash is greater than for the Oracle online database backup and recovery solution.

Note:

- The Oracle online database backup function can only perform a physical bit-for-bit backup of a single OpenPages with Watson database instance and only on one machine.
- Operation of online database backup in an Oracle RAC (cluster) environment is not supported.

In contrast, OPBackup performs a logical backup of all database instances in the cluster, as well as the OpenPages with Watson storage directory and application environment files.

Running Oracle online database backups (RMAN)

Setting up and running Oracle online database backups has several steps.

Complete the following steps to set up and run Oracle online database backups:

[“Plan the size of the Oracle backup area” on page 729](#)

[“Copying the online Oracle backup scripts to a local directory” on page 730](#)

[“Modifying the environment variables in the Oracle RMAN-ENV script” on page 730](#)

[“Configure the Oracle database for online backup” on page 732](#)

[“Run the Oracle rman-daily script” on page 733](#)

Plan the size of the Oracle backup area

The backup area is the location where the Oracle online database backup function stores the backup copy of the database instance plus the redo logs and other database-related files.

The online redo log represents the currently running incremental database backup, and the archived redo logs represent previous incremental backups. Estimate the maximum size of the backup area in order to set the appropriate environment variable. For more information, see [“Modifying the environment variables in the Oracle RMAN-ENV script” on page 730](#).

As a guideline, use a backup area that is 3x the size of the database. It includes the sum of the database, database copy, and archived log files.

The size of the backup area must be large enough to store all of the following information:

- A copy of the database instance
- All online redo logs
- Any archived redo logs that have not been backed up elsewhere.
- A copy of the database control file and the SPFILE

The backup area should be able to store at least 24 hours of archived redo logs that have not been backed up.

Copying the online Oracle backup scripts to a local directory

To access the scripts for online database backup, copy them from the installation media, OP_<version>_Main, to any local directory on the database server. You can run the scripts from the local directory.

Procedure

1. Log on to the IBM OpenPages with Watson database server as a user with administrative privileges.
2. Open a command or shell window.
3. Go to the following directory:
/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/
INSTALL_SCRIPTS
4. From the INSTALL_SCRIPTS directory copy, the following scripts to a local directory on the database server.

- Environment-specific online backup scripts:

Windows

```
rman-env.cmd  
rman-init.cmd  
rman-daily.cmd  
recover-db.cmd
```

Linux

```
rman-env.sh  
rman-init.sh  
rman-daily.sh  
recover-db.sh
```

- More online backup scripts:

```
enable-archivelog-mode.sql  
disable-archivelog-mode.sql  
check-fra-size.sql  
load_OP_APP_DATA.sql  
no-op.sql  
sql-wrapper.sql  
update-fra-size.sql  
init_recovery_env.sql
```

Note:

- The name of the local directory where you are copying the scripts must not contain any space characters.
- You can run the scripts described in the following topics from the local directory. You can add the directory to your PATH environment variable so that you can run them from any directory.

Modifying the environment variables in the Oracle RMAN-ENV script

After you determine the size of the backup area, edit the environment variable values in the rman-env script.

Before you begin

Complete the following steps to modify the Oracle RMAN-ENV script:

Procedure

1. Open the `rman-env.cmd` (Windows) or `rman-env.sh` (Linux) script in a text editor on the database server. Edit the following environment variables for your Oracle database environment as shown in Table 225 on page 731.

Table 225. Environment Variables in RMAN-ENV Script	
Environment Variable	Description
ORACLE_HOST_NAME=	Fully qualified network identifier for the database server computer. The host name can be found in the HOST parameter in the <code>tnsnames.ora</code> file. Example: <code>mydbhost.openpages.com</code>
ORACLE_SID=	SID of the IBM OpenPages database instance you are backing up. The SID can be found in the SERVICE_NAME parameter in the <code>tnsnames.ora</code> file. Example: <code>op</code>
ORACLE_HOME=	The Oracle database Home directory on the database server where the Oracle software is installed, including the database. This is the same as the value of the <code><ORACLE_HOME></code> environment variable for the database server. Examples Database and application servers on the same machine: Windows <code>C:\openpages_data\repository\server112_se_x64\software</code> Linux <code>/opt/oracle/openpages_data/repository/server112_se_x64/software</code> Database and application servers on different machines: Windows <code>C:\openpages_data\repository\client112_ac_x64\software</code> Linux <code>/opt/oracle/openpages_data/repository/client112_ac_x64/software</code>
ORACLE_DATAFILE_LOC=	The Oracle data Home directory on the database server. This is the location where the Oracle data is stored. Examples Windows <code>C:\openpages_data\repository\database112_se_x64\ordata\<server_name></code> Linux <code>opt/openpages_data/repository/database112_se_x64/ordata/<server_name></code>

Table 225. Environment Variables in RMAN-ENV Script (continued)	
Environment Variable	Description
FLASH_RECOVERY_AREA=	Directory or file system where the backup area will be located on the database server. Example: c:\temp\arch (Windows)
FLASH_RECOVERY_AREA_SIZE=	Maximum size of the backup area, specified in either megabytes (M) or gigabytes (G). You can specify any size up to the maximum allowed by the operating system on the database server. Examples: • 500M (500 megabytes) • 20G (20 gigabytes)
LISTENER_PORT=	Listener port number of the Oracle database instance you are backing up. The listener port number can be found in the PORT parameter in the tnsnames.ora file. Example: 1521
ORACLE_HOME_NAME=	Name assigned to <ORACLE_HOME> at installation time. The Oracle Home Name can be found in the SERVER parameter in the inventory.xml file in the <Oracle_Home>\Inventory\ContentsXML directory. Example: OPServer

2. Save the script file.

Results

After you enable online backup mode for a database instance, do not make any changes to the corresponding rman-env script. If you need to increase the size of the backup area, see "Adjusting the Size of the Backup Area" for more information. Never modify the rman-env script to adjust the size of the backup area after online database backup mode is enabled.

If you need to back up a different database instance, make a copy of the rman-env script in a different directory and modify the parameters as appropriate. The FLASH_RECOVERY_AREA parameter must specify a different location than that of your other online database backups.

Configure the Oracle database for online backup

Run the rman-init script to create the required directories and scripts for database recovery and to configure the parameters that you entered in the rman-env script for Oracle online database backup.

To run the script, execute the following command:

Windows

```
rman-init.cmd <tns_name_alias> SYS "<sysdba_password>"
```

Linux

```
rman-init.sh <tns_name_alias> SYS '<sysdba_password>'
```

Where:

<tns_name_alias> is the TNS alias of the IBM OpenPages with Watson database instance as it is known on the network. If necessary, you can retrieve this alias from the `tnsnames.ora` file.

<sysdba_password> is the Oracle SYS account password.

Windows example

```
rman-init op SYS "password"
```

If there are errors when running this script, the script output will list the directory location containing the error log. The error log file name is `enable-archivelog-more.log`.

Important: The script described in this section restarts the database. It is recommended that you alert users that they will be temporarily unable to access the database until the script has finished running.

Run the Oracle `rman-daily` script

The `rman-daily` script can be run manually or on a scheduled basis by using standard operating system scheduler functions (such as `cron`).

After you configure the database for online backup, you can run the `rman-daily` script to perform online backups.

Run the following command:

Windows

```
rman-daily.cmd <tns_name_alias> SYS "<sysdba_password>"
```

Linux

```
rman-daily.sh <tns_name_alias> SYS '<sysdba_password>'
```

Where:

<tns_name_alias> is the TNS alias of the IBM OpenPages with Watson database instance as it is known on the network. If necessary, you can retrieve this alias from the `tnsnames.ora` file.

<sysdba_password> is the Oracle SYS account password.

Linux example

```
rman-daily.sh op SYS 'password'
```

Review Oracle log files

The `rman-daily` script produces a log file (`rman-daily.log`) that lists each component that was backed up. The log is recreated (overwritten) each time that you run the `rman-daily` script.

The directory location of the `rman-daily.log` is:

Windows

<FLASH_RECOVERY_AREA>\<ORACLE_SID>\logs

Linux

<FLASH_RECOVERY_AREA>/<ORACLE_SID>/logs

Where:

<FLASH_RECOVERY_AREA> and <ORACLE_SID> are the values of those parameters in the `rman-env` script.

The log file lists the following information for the online database backup:

- Backup sets (incremental backups)
- Copies of data files

- Copies of control files
- Temp files

Monitoring the size of the Oracle backup area

You can use a script to monitor the size of the backup area.

To monitor and display the size of the backup area, use the following script:

```
sqlplus /nolog @sql-wrapper check-fra-size.sql <log_file_name> <tns_name_alias>
SYSTEM <system_password>
```

Where:

- <log_file_name> is the directory location, including the log file name that you specify, where any errors or messages relating to this script are logged. If you specify only the log file name, it is stored in the current working directory.
- <tns_name_alias> is the TNS alias of the IBM OpenPages with Watson database instance as it is known on the network. If necessary, you can retrieve this alias from the tnsnames.ora file.
- <system_password> is the Oracle SYSTEM account password.

If the password contains special characters, surround the password in quotation marks:

- Windows: "password"
- Linux: 'password'

The script displays the following information (in megabytes):

- Used Space — Space that is already used and not available for online database backups.
- Allocated Space — Maximum size of the backup area, including used and free space. This is the same as the value of the FLASH_RECOVERY_AREA_SIZE parameter in the rman-env script.
- Used-Reclaimable — Space that is free for use in online database backups.

Example: Displays the used, allocated, and free space for the database instance op.

- Windows:

```
sqlplus /nolog @sql-wrapper check-fra-size.sql C:\OpenPages\logs op SYSTEM "password"
```

- Linux:

```
sqlplus /nolog @sql-wrapper check-fra-size.sql /tmp/log op SYSTEM 'password'
```

Adjusting the size of the Oracle backup area

You can adjust the size of the backup area if necessary.

Occasionally, you may need to modify the size of the backup area. For example, you may see the following warning message in the Oracle Alert log:

```
ORA-19815: WARNING: db_recovery_file_dest_size of xxxxx bytes is 100.00% used,
and has 0 remaining bytes available
```

Increase the size of the backup area to make more space available for online database backups. You can increase or decrease the size of the backup area by running one of the scripts described in the following section.

Important: Do not delete files manually from the backup area to free up space. Doing so causes the following error: RMAN-06059: expected archived log not found.

Reclaiming used space by running the Oracle `rman-daily` script

Running the `rman-daily` script reclaims previously used space in the backup area, freeing it up for use in online database backups.

Adjusting space by running the Oracle `UPDATE-FRA-SIZE` script

You can adjust the size of the backup area by using a script.

If you want to adjust the maximum size of the backup area to a specific value, run the following scripts. The `enable-archivelog-mode.sql` script enables archive log mode, which enables Oracle online database backup for the specified database instance. The `update-fra-size.sql` script adjusts the size of the online backup area.

```
sqlplus /nolog @sql-wrapper enable-archivelog-mode.sql <log_file_name> <tns_name_alias>
sys <sysdba_password> <archive_dir> <file_size>
sqlplus /nolog @sql-wrapper update-fra-size.sql <log_file_name> <tns_name_alias>
SYS <sysdba_password> <new_size>
```

Where:

- `<log_file_name>` is the directory location, including the log file name that you specify, where any errors or messages relating to this script are logged. If you specify only the log file name, it is stored in the current working directory.
- `<tns_name_alias>` is the TNS alias of the IBM OpenPages with Watson database instance as it is known on the network. If necessary, you can retrieve this alias from the `tnsnames.ora` file.
- `<sysdba_password>` is the Oracle SYS account password.

If the password contains special characters, surround the password in quotation marks:

- Windows: "password"
- Linux: 'password'

- `<archive_dir>` is the directory where the archive file is stored.
- `<file_size>` is the maximum size of the archive file.
- `<new_size>` is the updated size of the backup area (use M for megabytes or G for gigabytes). For example, you would specify 20 gigabytes as 20G.

Example: Enables archive log mode and then sets the backup area for the database instance `op` to 1 gigabyte.

- Windows:

```
sqlplus /nolog @sql-wrapper enable-archivelog-mode.sql c:\tmp\log OP sys
"password" c:\tmp 50M
sqlplus /nolog @sql-wrapper update-fra-size.sql C:\temp\log op SYS "password" 1G
```

- Linux:

```
sqlplus /nolog @sql-wrapper enable-archivelog-mode.sql /tmp/log OP sys
'password' /tmp/ 50M
sqlplus /nolog @sql-wrapper update-fra-size.sql /tmp/log OP sys 'password' 1G
```

Important: The script restarts the database. Users are unable to access the database while the script is running.

Disabling online backup of the Oracle database instance

Run the following script to turn off archive logging mode, which disables Oracle online database backup for the specified database instance.

This simply stops the service that runs online database backup; it does not remove any files or data already stored in the backup area.

```
sqlplus /nolog @sql-wrapper disable-archivelog-mode <log_file_name> <tns_name_alias>  
SYS <sysdba_password>
```

Where:

- <log_file_name> is the directory location, including the log file name that you specify, where any errors or messages relating to this script are logged. If you specify only the log file name, it is stored in the current working directory.
- <tns_name_alias> is the TNS alias of the IBM OpenPages with Watson database instance as it is known on the network. If necessary, you can retrieve this alias from the `tnsnames.ora` file.
- <sysdba_password> is the Oracle SYS account password.

If the password contains special characters, surround the password in quotation marks:

- Windows: "password"
- Linux: 'password'

Example: Disables online backup for the database instance `op`.

- Windows:

```
sqlplus /nolog @sql-wrapper disable-archivelog-mode c:\tmp\log op SYS "password"
```

- Linux:

```
sqlplus /nolog @sql-wrapper disable-archivelog-mode /tmp/log op SYS 'password'
```

Important:

- The script restarts the database. Users are unable access the database while the script is running.
- After disabling online database backup mode, if you want to re-enable online database backup mode for the database instance, do not use the `rman-init` or `rman-daily` scripts. Doing so may cause unpredictable database behavior or other problems. To re-enable online database backup mode, contact IBM OpenPages Support for assistance.

Performing Oracle online database crash recoveries

If a system crash or other problem either corrupts the database instance or causes it to fail, the database must be recovered from the online backup.

The actual recovery procedure may vary depending on the nature of the crash, which parts of the database were damaged, and your system environment. For that reason, database recoveries must only be performed by IBM OpenPages Support.

Refreshing a test environment from backup files

To refresh an existing test (target) environment, you can replicate it from a production (source) environment. By using backup files from a production environment, you can update a test environment that closely matches your production environment.

Note: Oracle Data Pump backup files are created on the database server.

Prerequisites

Ensure you have access to the production server and test server.

Ensure the production server and test server have the same installed version of IBM OpenPages with Watson, including patches.

Ensure you have access to the installation media: `OP_version_Main`

Backing up and copying the OpenPages with Watson application production files for an Oracle database

The exported data from the production backup file will be used later to refresh data on the test server.

Procedure

1. Log on to your production IBM OpenPages with Watson server as a user with administrative permissions.
2. Run the OpenPages with Watson backup utility (OPBackup) to back up the OpenPages application database.
For more information, see [“The OPBackup utility” on page 682](#).
3. Copy the backup `.zip` or `.tar.gz` file to your test server.

Backing up the OpenPages with Watson application test files on your Oracle test data

You can back up IBM OpenPages with Watson application test data.

Procedure

1. Log on to your test OpenPages with Watson server as a user with administrative permissions.
2. Run the backup utility (OPBackup) as described in [“The OPBackup utility” on page 682](#) to backup the OpenPages with Watson application database.

Deleting data on the test database system

You can delete data on the test database system.

Procedure

1. If necessary, log on to your IBM OpenPages with Watson test server as a user with administrative permissions.
2. Open a command or shell window.
3. Go to the following directory:
`/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS`
4. From the `INSTALL_SCRIPTS` directory, run the `AuroraDbDelete.sql` script as follows:
 - a) Log on to SQL*Plus as the OpenPages with Watson database user (for example: `sqlplus openpages/openpages@test`).
 - b) Run the following script to drop the objects in the schema on the test server:
`@AuroraDbDelete.sql`
 - c) When finished, log out of SQL*Plus.

Copy the production database dump (.dmp) file to the test database server

You can copy the production database file to the test database server.

Procedure

1. Locate the database dump (.dmp) file directory on the source production and target test database servers.

Note:

To find the datapump directory for either the source or target database, run the following SQL query as the system user:

```
select directory_name, directory_path from dba_directories
where directory_name = upper ('OP_DATAPUMP_DIRECTORY');
```

By default, the datapump directory on the database server is <oracle-server-directory>|admin|<sid>|dpdump

2. Copy the IBM OpenPages with Watson database dump (.dmp) file from the Oracle datapump directory on the production database server to the datapump directory on the test database server.

Table 226. Default file name for .dmp file	
For this .dmp file...	The default file name will be similar to this...
OpenPages with Watson	OPENPAGES_<timestamp>.DMP

Note: Make sure to copy the .dmp file with the timestamp that matches when you ran the OPBackup command.

Import the production data into the test environment

You must import the IBM OpenPages with Watson database.

Procedure

1. Open a command or shell window and set the NLS_LANG environment variable as follows.

Windows

In the Command Prompt window where you will be invoking the import commands, execute the following command:

```
set NLS_LANG=AMERICAN_AMERICA.AL32UTF8
```

Linux

Open the .profile file in the logged in user's home directory in a text editor and enter the following line if it is missing in the file:

```
export NLS_LANG=AMERICAN_AMERICA.AL32UTF8
```

Save the change to the file, and either execute the .profile in your shell window or log on again.

2. Import the OpenPages database on the test database server from the backup files in “Backing up and copying the OpenPages with Watson application production files for an Oracle database” on page 737 as follows.

Note: The Oracle Data Pump command IMPDP is used as the IMP command is not supported.

For more information on Oracle Data Pump, see “Oracle Data Pump” on page 713.

From the same command or shell window, run the following command to import the OpenPages database:

```
impdp <op_db_user>/\"<op_db_password>\"@<SID>
DIRECTORY=OP_DATAPUMP_DIRECTORY DUMPFILE=<openpages_dump_file>
LOGFILE=openpages_import.log
```

Table 227. Parameters and their descriptions	
Parameter	Description
<op_db_user>	The user name for accessing the OpenPages database.
<op_db_password>	The password for accessing the OpenPages database.
<SID>	The Oracle System Identifier (for example, OP or OP).
<openpages_dump_file>	The .dmp file name of the backed up OpenPages with Watson application database. Important: Do not enter an explicit path when specifying the .dmp file name. Enter only the file name.
DIRECTORY	The directory on the database server where the backed up files will be placed. This is set when “Configuring or updating the Oracle Data Pump directory” on page 725. Important: Do not enter an explicit path when specifying the DIRECTORY parameter. Use OP_DATAPUMP_DIRECTORY only.

Example

```
impdp openpages/\"openpages\"@OP
  DIRECTORY=OP_DATAPUMP_DIRECTORY DUMPFILE=openpages_backup_YYYY_MM_DD_HH_MI_SS.dmp
  LOGFILE=openpages_import.log
```

Note: If the source schema name and target schema names are different, the schema must be remapped during import. Add the following argument to this impdp command to remap the schema:

```
Remap_schema=<source_schema>:<target_schema>
```

Example

```
impdp openpages/\"openpages\"@OP
  DIRECTORY=OP_DATAPUMP_DIRECTORY DUMPFILE=openpages_backup_YYYY_MM_DD_HH_MI_SS.dmp
  LOGFILE=openpages_import.log remap_schema=opuser:openpages
```

Update the OpenPages with Watson storage location in the Oracle database

After you restore the **openpage-storage** file from the product backup, you must update the IBM OpenPages with Watson storage location in the database.

Procedure

1. Log on to a system with administrative permissions. You can use any system with access to CLPPlus that can connect to the OpenPages database server.
2. Copy all the files under the openpages-storage folder from the production backup .zip file to the openpages-storage location on the test server.

By default, the storage location is <OP_Home>|openpages-storage

Table 228. Installation location of the OpenPages with Watson application	
Operating system	Installation location
Windows	For example, <OP_Home> C:\IBM\OpenPages
Linux	For example, <OP_Home> /opt/IBM/OpenPages

3. Open a command or shell window and go to the following directory:

```
/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/
INSTALL_SCRIPTS
```

4. From the INSTALL_SCRIPTS directory, run the update-storage SQL wrapper script with the following parameters (see Table 229 on page 740 for a description) to update the openpages-storage directory location in the database:

```
sqlplus /nolog @sql-wrapper.sql update-storage <log-file> <oracle_tns_alias>
<op_db_user> <op_db_password> <storage-type> <storage-server-name>
<host-name> <os-type> <path-or-UNC-name>
```

Where:

Table 229. Update Storage Wrapper Script Parameters	
Parameter	Description
<log-file>	The name of the log file that the script will create and write information to.
<oracle_tns_alias>	The database alias for the OpenPages with Watson database instance, as set during the Oracle database installation.
<op_db_user>	The OpenPages with Watson user name for accessing the OpenPages with Watson database.
<op_db_password>	The OpenPages with Watson password for accessing the OpenPages with Watson database. If the password contains special characters, surround the password in quotation marks: • Windows: "password" • Linux: 'password'
<storage-type>	The type of file storage to be used. Valid values are: • LFS (local file system) • UNC (Universal Naming Convention) Note: After you move from LFS to UNC, you cannot go back to using LFS.
<storage-server-name>	The name of the storage server.
<host-name>	The host name of the machine.
<os-type>	The type of operating system. Valid values are: • Windows • Unix
<path-or-UNC-name>	The file path or UNC of the storage location.

Examples

- LFS

Windows

```
sqlplus /nolog @sql-wrapper.sql
update-storage c:\temp\upd-storage-output.log
op openpages "password" LFS eng11 eng11
Windows c:\OpenPages\openpages-storage
```

Linux

```
sqlplus /nolog @sql-wrapper.sql
update-storage /home/op/upd-storage-output.log
op openpages 'password' LFS eng11 eng11
Unix /usr/opdata/openpages-storage
```

- UNC

Windows

```
sqlplus /nolog @sql-wrapper.sql
update-storage c:\temp\update-storage-output.log
op openpages "password" UNC eng11
eng11 Windows openpages-storage
```

Update the global search settings

After you import data from a production environment (the source environment) into a test or development environment (the target environment), you need to update the global search settings.

About this task

When you import data from the source environment, the settings for the search server are imported. You need to update the target environment so that it uses the search server in your target environment.

Procedure

1. Log in to the OpenPages application in the target environment as a user with administrative privileges.
2. If the global search component is enabled, disable it.
 - a) Click **Administration > Global Search**.
 - b) Click **Disable**.
3. Stop the global search services.

For more information, see [“Start or stop the global search services” on page 844](#).

4. Update the global search settings.
 - a) Click **Administration > Settings > Applications > Common > Configuration > Show Hidden Settings** and set the value to true.
 - b) Click **Administration > Settings > Platform > Search > Admin** and update the **Search Server Administration URL** with the URL of the search server in your target environment.
 - c) Click **Administration > Settings > Platform > Search > Index** and update the **Search Server URL** with the URL of the search server in your target environment.
 - d) Click **Administration > Settings > Platform > Search > Request** and update the **Search Server URL** with the URL of the search server in your target environment.
5. Copy the <SEARCH_HOME>/openpages-solr-index directory to the search server in the target environment.

The <SEARCH_HOME>/openpages-solr-index contains the global search index.

6. Start the global search services.

For more information, see [“Start or stop the global search services” on page 844](#).

7. Enable global search. Click **Administration > Global Search > Enable**.

Results

Global search is enabled in the target environment.

Update Cognos data in the test environment

You can update Cognos data in the test environment by using the Cognos backup utility.

Before you begin

Before you run the Cognos backup utility (OPCCBackup) make sure to verify the following:

- You have access to both the source and target database servers.
- The <CC_user> has Read and Write permission to the OP_DATAPUMP_DIRECTORY.

Where: <CC_user> is the name of the Cognos content store database user.

If not, you must grant the proper permissions on both the production and test servers to the <CC_user> account on the datapump directory as follows:

1. Log on to a machine with SQL*Plus and access to the database server.
2. Run the following SQL command as the system user:

```
grant read,write on directory OP_DATAPUMP_DIRECTORY to <CC-user>;
```

- Full permission is granted to the CommandCenter\tools\bin folder on the target Cognos server.

Backup Cognos production Oracle data and files

The exported data from the production backup file will be used later to refresh data on the test server.

Procedure

1. If necessary, log on to your production Cognos server as a user with administrative permissions.
2. Run the Cognos backup utility (OPCCBackup) to back up the Cognos database and configuration files.

For more information, see [“Using the Cognos backup utility” on page 724](#).

Tip: If the mail server for notification e-mails has not been set up for running Cognos backups, the output from the OPCCBackup command might end with the following error:

```
BUILD FAILED
c:\machine3\CommandCenter\tools\bin\op-cc-backup-email-notification.xml:31:
  Problem while sending mime mail:
```

This error can be safely ignored as long as this step says BUILD SUCCESSFUL.

3. Copy the production Cognos server backup .zip or .tar.gz file to the Cognos backup-restore directory on the test server.
4. Copy the database dump (.dmp) file from the Oracle datapump directory on the source database server to the datapump directory on the target database server.

Make sure you copy the dump file with the timestamp that matches when you ran the OPCCBackup command. By default, the file will be named similar to OPENPAGES_CC_<timestamp>.DMP.

Note:

To find the datapump directory for either the source or target database, run the following SQL query as the system user:

```
select directory_name, directory_path from dba_directories
where directory_name = upper ('OP_DATAPUMP_DIRECTORY');
```


By default, the datapump directory on the database server is <oracle-server-directory>|admin|<sid>|dpdump

Backing up the Cognos Oracle test data and files

You can back up test data and files.

Procedure

1. If necessary, log on to your test IBM OpenPages with Watson server as a user with administrative permissions.
2. Run the Cognos backup utility (OPCCBackup) as described in “Using the Cognos backup utility” on page 724 to back up the Cognos database and configuration files.

Restoring the Cognos data and files to the Oracle test environment

You can restore data and files to the test environment.

Procedure

1. Log on to your test IBM OpenPages with Watson server as a user with administrative permissions.
2. From the INSTALL_SCRIPTS directory, run the AuroraDbDelete.sql script as follows:
 - a) Log on to SQL*Plus as the Cognos database user (for example: sqlplus cognos/cognos@test).
 - b) Run the following script to drop the objects in the schema on the test server:
@AuroraDbDelete.sql
 - c) When finished, log out of SQL*Plus.
3. Import the Cognos database on the target (test) database server from the backup file from the source (production) database server as follows.

From a command or shell window, run the following command to import the Cognos database:

```
impdp <cognos_db_user>/\"<cognos_db_password>\"@<SID>  
DIRECTORY=OP_DATAPUMP_DIRECTORY  
DUMPFILE=<cc_dump_file> LOGFILE=cc_import.log
```

Where:

Table 230. Parameters and their descriptions	
Parameter	Description
<cognos_db_user>	The Cognos user name for accessing the Cognos database.
<cognos_db_password>	The Cognos password for accessing the Cognos database.
<SID>	The Oracle System Identifier (for example, OP).
<cc_dump_file>	The .dmp file name of the backed up Cognos database.

Example

```
impdp cognos/\"cognos\"@OP DIRECTORY=OP_DATAPUMP_DIRECTORY  
DUMPFILE=openpages_cc_YYYY_MM_DD_HH_MI_SS.dmp  
LOGFILE=openpages_cc_import.log
```

Note: If the source schema name and target schema names are different, the schema must be remapped during import. Add the following argument to this impdp command to remap the schema:

```
Remap_schema=<source_schema>:<target_schema>
```

Example

```
impdp cognos/"cognos"@OP DIRECTORY=OP_DATAPUMP_DIRECTORY  
DUMPFILE=openpages_cc_YYYY_MM_DD_HH_MI_SS.dmp  
LOGFILE=openpages_cc_import.log remap_schema=cognos8:cognos
```

Change password references for Oracle data sources

The following procedure describes how to manually update the signon password for the user account to access data sources.

Depending on the type of installation, one or both of the following Oracle data source links are displayed in the IBM Cognos Administration tool for the reporting framework:

- The **OpenPages DataSource** is used for the Reporting Framework V6. V6 refers to the latest framework version, not to any specific OpenPages release number.

Note: For Oracle Database environments only, both the **OpenPages DataSource** and **Oracle Native Driver** data sources connect to the same database repository and use the same authentication information (signons).

Procedure

1. From a browser, log on to the IBM Cognos Analytics as a user with administrative privileges, for example, OpenPagesAdministrator.
By default, the URL is `http://<hostname>/ibmcognos/bi`
Where <hostname> is the name of the Cognos server.
2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Configuration** tab, click **Data Source Connections** (if not already selected).
4. On the **Directory > Cognos** page, click the **More** link in the same row as the data source you want (for example, OpenPages DataSource).
5. On the **Perform an Action** page, under **Available actions**, click the **View connections** link.
6. On the **Directory > Cognos > < name of data source >** page, click the **More** link in the same row as the selected data source.
7. On the **Perform an Action** page for the data source, under **Available actions**, click the **View signons** link.
8. On the **Directory > Cognos > < name of data source > signons** page, do the following:
 - a) Under the **Actions** column, click the **Set properties - < name of data source >**  icon.
 - b) On the **Set properties-< name of data source >** page, click the **Signon** tab.
9. On the **Signon** tab:
 - a) Click the **Edit the signon** link.
 - b) Update the password.

Updating Oracle database connection references for reports

You can update the database connection references for reports.

Procedure

1. From a browser, log on to the IBM Cognos Analytics as a user with administrative privileges, for example, OpenPagesAdministrator.

By default, the URL is:

`http://<hostname>/ibmcognos/bi` (if you are using port 80 for Cognos)

Where <hostname> is the name of the Cognos server.

2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Configuration** tab, click **Data Source Connections** (if not already selected).
4. On the **Directory > Cognos** page, click the link for the IBM OpenPages with Watson data source.
5. On the **Directory > Cognos > OpenPages DataSource** page, do the following:
 - a) Under the **Actions** column, click the **Set properties - OpenPages DataSource** icon .
 - b) On the **Set properties - OpenPages DataSource** page, click the **Connection** tab.
6. On the **Connection** tab, next to the **Connection String** box, click the pencil icon to edit the field.
7. On the edit page, do the following:
 - a) On the **OCI** tab, in the **SQL*Net connect string** box, change the SQL*Net connect string to the TNS alias of the OpenPages database on the target environment.
 - b) On the **JDBC** tab, in the **Server name**, **Port number**, and **Oracle Service ID** boxes, change the values to valid values for the IBM OpenPages with Watson database on the target environment.
8. If this is an upgraded legacy system, repeat the steps in this task for the Oracle Native Driver, if it exists.

Modify SSO and LDAP Configuration in the test environment

If you are using SSO and/or LDAP in the test environment, modify the configuration for each if needed. Otherwise, skip this task.

Copy custom triggers

You must copy any custom Java actions and triggers that have been deployed on the production server to the test environment. These custom actions and triggers are added to a zip file, `openpages-ext.jar`, by the OPBackup utility.

If you have any questions about the location of your custom data, contact IBM OpenPages Support.

Procedure

1. If necessary, log on to your test IBM OpenPages with Watson server as a user with administrative permissions.
2. Update the `openpages-ext.jar` in the test environment as follows:
 - a) From the production backup .zip file, navigate to the `openpages-ext.jar` in the `<OP_Home>|aurora|lib` directory.

Where `<OP_HOME>` represents the installation location of the IBM OpenPages application.

Table 231. Installation location of the OpenPages with Watson application	
Operating system	Installation location
Windows	<code><OP_HOME>\aurora\lib\openpages-ext.jar</code> By default <code><OP_HOME></code> is <code>C:\IBM\OpenPages</code>

Table 231. Installation location of the OpenPages with Watson application (continued)	
Operating system	Installation location
Linux	<OP_HOME>/aurora/lib/openpages-ext.jar By default <OP_HOME> is /opt/IBM/OpenPages

- b) Copy the openpages-ext.jar from the production backup file into the <OP_Home> | aurora | lib directory on your test machine and overwrite the existing .jar file there.

Copy other custom deliverables to the test environment

If you have other custom deliverables, such as UI helpers and JSP reports, copy these custom deliverables to their respective folders on the test or target machine.

If you have any questions about the location of your custom data, contact IBM OpenPages Support.

Procedure

1. From your application production backup .zip files, extract all custom files such as JAR files, JSP files, JavaScript files, and Image files.
2. Copy these files into their respective folders on the target machine. The target folders should match the folders on the source installation.

Starting the OpenPages with Watson in the test environment

When finished, start IBM OpenPages with Watson services on the servers in your test environment.

For details, see [Chapter 24, “Starting and stopping servers,” on page 841](#).

Updating the OPSysSystem password

If the OPSysSystem password is different in the source (production) and target (test) environments or if you changed the default OPSysSystem password, update the OPSysSystem password in the test environment.

For more information, see [“Changing the OPSysSystem password” on page 773](#).

Update URL host pointers for Cognos reports

Modify the URL host pointer settings and then propagate these changes to the reporting schema on the application server (does not require services to be restarted).

For more information, see [“Updating URL host pointers for reports” on page 769](#).

Utilities for filtering on long string field content in an Oracle database

You can filter based on the content of long string fields if the Oracle Text feature has been enabled. This is also known as full text searching.



Warning: Do not include long string fields that are encrypted using field level encryption in the search criteria because they can return unexpected results.

Long string fields allow users to enter values over 4KB in length. To apply filters on the content of these long string fields, first [“Enabling Oracle Text” on page 748](#) feature. If the Oracle Text feature is not enabled, attempts to filter on the content of long string fields will generate errors. For details on setting up long text fields, see [“Long String data type” on page 204](#).

There are five utilities provided to help manage full text searching:

- “Enabling Oracle Text” on page 748
- “Create a long string index for an Oracle database” on page 747
- “Create a schedule job to synchronize a long string index” on page 749
- “Drop a long string index” on page 750
- “Modifying the list of stop words” on page 751

To apply filters with long string fields, you must change the **OpenPages > Platform > Database > Text Indexes** setting to **true**.

Table 232. Values and what they mean	
If the value is set to...	Then...
true	Filtering is enabled on long string fields.
false	Filtering is disabled on long string fields. The default is false .

For details on working with settings, see [Chapter 19, “Viewing the Configuration and Settings page,”](#) on page 597.

Create a long string index for an Oracle database

Create a long string text index to support filtering based on the contents of fields with long string data types. Scripts are provided for both Windows and Linux.

Before you begin

Oracle Text must be enabled. See [“Enabling Oracle Text”](#) on page 748.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the IBM OpenPages with Watson database server.
2. Open a command or shell window, navigate to the full-text-index directory as follows.

The following table identifies the installation location of the application on the Microsoft Windows and Linux operating systems.

Table 233. Installation location of the full-text-index directory	
Operating system	Installation location
Windows	<OP_HOME>\aurora\bin\full-text-index
Linux	<OP_HOME>/aurora/bin/full-text-index

Note: If the database server is not on the same computer as the OpenPages server, you must copy the script, and the SQL files it starts, to the database server.

3. Run the following batch command:

Windows

```
CreateOpenPagesTextIndex.bat <SID> <OPX_USER_NAME>  
"<OPX_USER_PASSWORD>" <MEMORY_LIMIT> <PARALLEL_INDEXING_DEGREE>
```

Linux

```
CreateOpenPagesTextIndex.sh <SID> <OPX_USER_NAME>
```

```
'<OPX_USER_PASSWORD>' <MEMORY_LIMIT> <PARALLEL_INDEXING_DEGREE>
```

Table 234. Parameters	
Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<OPX_USER_NAME>	OpenPages database schema owner name.
<OPX_USER_PASSWORD>	OpenPages database schema owner password.
<MEMORY_LIMIT>	Specifies the amount of runtime memory to use for indexing, in megabyte or gigabyte values. For example, valid values include 128M and 2G.
<PARALLEL_INDEXING_DEGREE>	Parallel degree for parallel indexing. The actual degree of parallelism might be smaller depending on system resources.

Enabling Oracle Text

Enable the Oracle Text feature to filter based on the contents of fields with long string data types. Scripts are provided for Windows and Linux.

Procedure

1. Log on to the Oracle database server as a user with database administrator privileges.

Note: You can enable only Oracle Text from the database server.

2. Open a command or shell window, navigate to the `full-text-index` directory as follows.

The following table identifies the installation location of the application on the Microsoft Windows and Linux operating systems.

Table 235. Installation location of the full-text-index directory	
Operating system	Installation location
Windows	<OP_HOME>\aurora\bin\full-text-index
Linux	<OP_HOME>/aurora/bin/full-text-index

Note: If the database server is not on the same computer as the IBM OpenPages with Watson server, copy the script and the SQL files to the database server.

3. Run the following batch command:

Windows

```
EnableOpenPagesTextIndexing.bat <SID> <SYSDBA_USER_NAME>  
"<SYSDBA_PASSWORD>" <OPX_USER_NAME>
```

Linux

```
EnableOpenPagesTextIndexing.sh <SID> <SYSDBA_USER_NAME>  
'<SYSDBA_PASSWORD>' <OPX_USER_NAME>
```

Note: All parameters are required.

Table 236. Parameters in the batch command	
Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages with Watson database instance.
<SYSDBA_USER_NAME>	Database SYSDBA account. Usually the SYS user.
<SYSDBA_PASSWORD>	Password for the SYSDBA user account.
<OPX_USER_NAME>	OpenPages with Watson application schema owner name.

Results

The database is now enabled for indexing. Use [“Create a long string index for an Oracle database” on page 747](#) script to create the index.

Create a schedule job to synchronize a long string index

Create a schedule to synchronize the long string index. Scripts are provided for both Windows and Linux.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the IBM OpenPages with Watson database server.
2. Open a command or shell window, then navigate to the `full-text-index` directory as follows.

The following table identifies the installation location of the application on the Microsoft Windows and Linux operating systems.

Table 237. Installation location of the full-text-index directory	
Operating system	Installation location
Windows	<OP_HOME>\aurora\bin\full-text-index
Linux	<OP_HOME>/aurora/bin/full-text-index

Note: If the database server is not on the same machine as the OpenPages server, you must copy the script, and the SQL files it invokes, to the database server.

3. Run the following batch command:

Windows

```
ManageOpenPagesTextIndexRefreshJob.bat <SID> <OPX_USER_NAME>
"<OPX_USER_PASSWORD>" <START_JOBS_AFTER_DAYS> <JOB_START_HOUR> <REFRESH_FREQ_IN_HOURS>
<REFRESH_FREQ_IN_MINS> <MEMORY_LIMIT> <PARALLEL_INDEXING_DEGREE> <MAX_SYNC_TIME>
```

Linux

```
ManageOpenPagesTextIndexRefreshJob.sh <SID> <OPX_USER_NAME>
'<OPX_USER_PASSWORD>' <START_JOBS_AFTER_DAYS> <JOB_START_HOUR> <REFRESH_FREQ_IN_HOURS>
<REFRESH_FREQ_IN_MINS> <MEMORY_LIMIT> <PARALLEL_INDEXING_DEGREE> <MAX_SYNC_TIME>
```

Table 238. Parameters	
Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<OPX_USER_NAME>	OpenPages database schema owner name.

Table 238. Parameters (continued)	
Parameter name	Description
<OPX_USER_PASSWORD>	OpenPages database schema owner password.
<START_JOBS_AFTER_DAYS>	Number of days between today and the scheduled starting date of the job. For example, 0 for today, 1 for tomorrow.
<JOB_START_HOUR>	The hour (on a 24-hour clock) of the scheduled starting date of the job. For example, 18 for 1800 hours or 6 p.m.
<REFRESH_FREQ_IN_HOURS>	Intervals (in hours) between each job. This value is combined with <REFRESH_FREQ_IN_MINS> value. Maximum of combined values is 999.
<REFRESH_FREQ_IN_MINS>	Intervals (in minutes) between each job. This value is combined with <REFRESH_FREQ_IN_HOURS> . Maximum of combined values is 999.
<MEMORY_LIMIT>	Specifies the amount of runtime memory to use for indexing, in megabyte or gigabyte values. For example, valid values include 128M and 2G.
<PARALLEL_INDEXING_DEGREE>	Parallel degree for parallel indexing. The actual degree of parallelism might be smaller depending on system resources.
<MAX_SYNC_TIME>	Maximum time (in minutes) the index synchronization job can run.

Results

Index synchronization jobs run at the interval specified.

Note: Changes to long string fields are not available for filtering until the next scheduled index job runs.

For example, `ManageOpenPagesTextIndexRefreshJob.bat OP opadmin "opadmin" 1 3 24 0 2G 0 60` schedules indexing synchronization to start at 3 AM, starting on the next day, and then repeats every day at the same time. There is a 2-gigabyte memory limit, no parallel indexing, and the job can run no more than an hour.

Drop a long string index

Remove the long string index. An index must be dropped before it can be recreated. Scripts are provided for both Windows and Linux.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the IBM OpenPages with Watson database server.
2. Open a command or shell window, then navigate to the `full-text-index` directory as follows.

The following table identifies the installation location of the application on the Microsoft Windows and Linux operating systems.

Table 239. Installation location of the full-text-index directory	
Operating system	Installation location
Windows	<OP_HOME>\aurora\bin\full-text-index
Linux	<OP_HOME>/aurora/bin/full-text-index

Note: If the database server is not on the same machine as the OpenPages server, you must copy the script, and the SQL files it invokes, to the database server.

3. Run the following command:

Windows

```
DropOpenPagesTextIndex.bat <SID> <OPX_USER_NAME> "<OPX_USER_PASSWORD>"
```

Linux

```
DropOpenPagesTextIndex.sh <SID> <OPX_USER_NAME> '<OPX_USER_PASSWORD>'
```

Table 240. Parameters	
Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<OPX_USER_NAME>	OpenPages database schema owner name.
<OPX_USER_PASSWORD>	OpenPages database schema owner password.

What to do next

You must recreate the index before filtering on the content of long string fields again. For details on creating a long string index, see [“Create a long string index for an Oracle database” on page 747](#).

Modifying the list of stop words

You can change the default list of stop words used by the Oracle Text feature. A stop word is a word that does not get indexed. When querying an Oracle Text index for a stop word, Oracle Text won't return data for the query.

By default, the `CreateOpenPagesTextIndex.bat | .sh` script creates a stop word list called `OP_STOPLIST`. (See [“Create a long string index for an Oracle database” on page 747](#).) The stop word list is empty at the time of index creation.

You can use the `CustomIndexing_ManageStopWords.sql` script to add stop words to `OP_STOPLIST`.

Procedure

1. Open `CustomIndexing_ManageStopWords.sql` with a text editor
2. Add a stop word for each word you would like to add by copying the following, commented out sections:

```
/*
  ADD_STOPWORD_TO_ARRAY
  (
    p_name          => 'me'
  );
*/
```

For example, if you want to add the stop word "the", copy the preceding section, remove the comment sign, and replace "me" with "the" as follows. Repeat the same step for each word you want to add.

```
ADD_STOPWORD_TO_ARRAY
(
  p_name          => 'the'
);
```

Stop words that you add to this file take effect the next time that you re-index. This file is used as the most updated list of stop words when the index is recreated. When running CustomIndexing_Step2_IndexCreate.sql, all current stop words in OP_STOPLIST are removed. It is a good idea to keep this file up to date.

String concatenation utility

String concatenation lets you merge up to 8 simple strings into a new long text field (long string data type). Long text fields have two sub categories - medium long and large long. Medium long can support a text size up to 32KB.

To concatenate simple strings, the fields must be unencrypted. After you use the concatenation utility, you can encrypt the new long text field.

You must log in as an administrator to perform string concatenation. You can use any system with access to SQL*Plus that can connect to the IBM OpenPages with Watson database server.

String concatenation is a database operation. A SQL template file is provided to specify parameters for the action. For more information, see [“Running string concatenation” on page 752](#).

For more information on long text fields, see [“Long String data type” on page 204](#).

Running string concatenation

The string concatenation utility runs an SQL file that you edit to provide input and output parameters.

Important:

- The string concatenation utility puts the system into System Administration Mode (SAM) prior to concatenating any fields. No other activity can happen while the script is running.
- You can concatenate into an existing long text field, but only if that field has not been used in any way. Attempting to concatenate into a long text field that has been used causes the utility to fail.
- When you concatenate multiple strings, if field level security is applied to any of the strings, then after concatenation into a single, large long text field, some hidden values can be visible. To prevent unauthorized users from viewing the values for a concatenated string, apply the same field level security rule to the large long text field.

Tip: Run the script in preview mode (a setting in the field_concat_template.sql file) to check the results before doing the concatenation.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the IBM OpenPages with Watson database server.
2. Stop all services (see [Chapter 24, “Starting and stopping servers,” on page 841](#)).
3. Navigate to the field-concat-utility folder located in the bin directory:

Table 241. Installation locations	
Operating system	Installation location
Windows	<OP_HOME>\aurora\bin
Linux	<OP_HOME>/aurora/bin

4. Copy the contents of the SQL template `field_concat_template.sql` into a new file.
5. Edit the new SQL file to provide the values necessary. Edit only the values in the declaration section of the SQL file. For details, see [“The string concatenation SQL file” on page 754](#).

Important: Many of the parameters specified in the SQL file have requirements, restrictions, and cautions noted. These are important for a successful concatenation.

Tip: When editing your copy of the `field_concat_template.sql` file with multi-byte characters, and saving the file in Unicode, your editor may insert a Byte Order Mark (BOM) into the file. Some applications (such as a text editor or a browser) display the BOM as an extra line in the file, while others display unexpected characters, such as `ï»¿`. If you save the file in UTF-8 encoding (leaving the BOM in the file) and run the string concatenation script, you get an error message (SP2-0734: unknown command beginning "`ï»¿-----...`"), but the script continues to run without a problem. This error has no effect on the script running, but if you prefer not to see the error, save the file without a Byte Order Mark.

6. Run the following command:

Windows

```
field_concat <SID> <op_db_user> "<op_db_password>"
<field_concat_template_file>
```

Linux

```
field_concat.sh <SID> <op_db_user> '<op_db_password>'
<field_concat_template_file>
```

Table 242. Parameters	
Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<username>	The OpenPages database schema user name.
<password>	The OpenPages database schema owner password. If the password contains special characters, surround the password in quotation marks: • Windows: "password" • Linux: 'password'
<field_concat_template_file>	The name of the SQL file created in step 3.

Tip: To see details on database operation messages, run the following SQL statement:

```
select exception_text from error_messages where
ERROR_MESSAGE_ID = &ERROR_MESSAGE_ID;
```

7. Start all services (see [Chapter 24, “Starting and stopping servers,” on page 841](#)).
8. Optional: Apply a field level security rule to the large long text field. For more information, see [“Field level security” on page 133](#).

Results

If the destination long text field does not exist, it is created and populated with values according to the values specified in the SQL file.

If the destination long text field exists, but is not used in any way, it is populated with values according to the values specified in the SQL file.

For details on the SQL file, see [“The string concatenation SQL file” on page 754](#).

The string concatenation SQL file

IBM OpenPages with Watson includes a template SQL file (`field_concat_template.sql`). Use a copy of this file to specify the parameters to submit with the `field_concat` command.

Important: Many of the parameters specified in the SQL file have requirements, restrictions, and cautions noted. These are important for a successful concatenation.

See [“Running string concatenation” on page 752](#).

Parameters

Table 243. <i>field_concat_template.sql</i> parameters	
Parameter	Description
<code>l_actor_name</code>	The user name making the change. The user must log in as an administrator. The script puts the system into System Administration Mode (SAM) prior to concatenating any fields.
<code>l_field_group_name_src<#></code>	The name of the field group containing the simple string field. Where: <code><#></code> is a value from 01 to 08. • <code>l_field_group_name_src<#></code> and <code>l_property_name_src<#></code> are always specified in pairs. • These parameters must have values specified in order. For example, <code>l_field_group_name_src01</code> must have a value before <code>l_field_group_name_src02</code> is specified. • Specified field groups must be associated with an object type.
<code>l_property_name_src<#></code>	The name of the source simple string field. Where: <code><#></code> is a value from 01 to 08. • The source must be a simple string. • At least one source must be specified. • The source must already exist • <code>l_field_group_name_src<#></code> and <code>l_property_name_src<#></code> are always specified in pairs. • These parameters must have values specified in order. For example, <code>l_property_name_src01</code> must have a value before <code>l_property_name_src02</code> is specified. • A property can only be specified once in the set of fields to concatenate. • Only the resource description system property is supported.

Table 243. *field_concat_template.sql* parameters (continued)

Parameter	Description
<code>l_separator</code>	The separator to use between concatenated fields. The default separator is null. If you concatenate only one source into the destination, the separator character is not used. - To use "&" as a separator, encode it as <code>chr(38)</code>. For example: <pre>l_separator OP_GLOBALS.DB_Max_String_T := chr(38);</pre> - The separator string can be no longer than 100 bytes. - If the destination field has a rich text display type, characters in the separator sequence must be encoded. For example, to represent a less-than sign ("<"), encode it as: <pre>l_separator OP_GLOBALS.DB_Max_String_T := chr(38) 'lt ';</pre>
<code>l_object_type_name</code>	The name of the object type containing the destination long text field. The object type must be the same for the destination as it is for the source.
<code>l_field_group_name</code>	The name of the field group containing the destination long text field. - The destination field group must exist. - The destination field group must be a customer field group, not a system field group.
<code>l_property_name</code>	The name of the destination field. - The name destination field must either not exist, or if it does exist, must not used anywhere. - If the destination field does not already exist, the <code>l_large_text_length</code> parameter must be specified. - If the destination field does exist, it must be of data type <code>Long String</code>. - If the destination field is Rich Text, and source fields are a mix of Text and Rich Text, then there is the possibility that the concatenated value will not display properly in the UI. Such operations should be executed with caution.
<code>l_property_desc</code>	The description of the destination long text field.

Table 243. *field_concat_template.sql* parameters (continued)

Parameter	Description
<code>l_large_text_length</code>	The length property of the destination field. The default is <code>OP_OBJ_MODEL_MGR.g_d1_longtext_medium</code>. If the destination does not exist, this parameter must be specified, as either <code>OP_OBJ_MODEL_MGR.g_d1_longtext_medium</code> or <code>OP_OBJ_MODEL_MGR.g_d1_longtext_large</code>.
<code>l_is_done_by_vendor</code>	Set to true to add the concatenation to audit trail. The default is <code>OP_Globals.sc_False</code>. Valid values are: • <code>OP_Globals.sc_True</code> • <code>OP_Globals.sc_False</code> See “Auditing configuration changes” on page 770
<code>l_remote_address</code>	The remote address to perform the audit trail. The default is null. Any value is ignored if <code>l_is_done_by_vendor</code> is <code>OP_Globals.sc_False</code>.
<code>l_remote_host</code>	The remote host to perform the audit trail. The default is null. Any value is ignored if <code>l_is_done_by_vendor</code> is <code>OP_Globals.sc_False</code>.
<code>l_preview_only</code>	Set to true to only print the changes that will be made by script. No changes are actually made. The default is <code>OP_Globals.sc_False</code>. Valid values are: • <code>OP_Globals.sc_True</code> • <code>OP_Globals.sc_False</code> Tip: Run the script in preview mode (a setting in the <code>field_concat_template.sql</code> file) to check the results before doing the concatenation.

Table 243. *field_concat_template.sql* parameters (continued)

Parameter	Description
<code>l_override_objtp_logic</code>	Set to true to override any logic applied to the object types, such as their relationships. The default is <code>OP_Globals.sc_False</code>. Valid values are: • <code>OP_Globals.sc_True</code> • <code>OP_Globals.sc_False</code> If <code>l_object_type_name</code> is left blank, and the source and destination field groups are associated to different object types, the script will fail unless you set this parameter to <code>OP_Globals.sc_True</code>. Each source field group and destination field group must associate with the same object type or set of object types. For example, the following scenario will fail unless this parameter is set to <code>OP_Globals.sc_True</code>: • Source field group A is associated to object types X and Y. • Source field group B is associated only to object type X. • Destination field group is associated only to object type X.

Sample

Note: The following sample includes only those declarative statements that are subject to your changes.

```

declare
  l_actor_name          ACTORINFO.NAME%type           := 'OPAdmin';
  l_field_group_name_src01 BUNDLEDEFS.NAME%type       := 'QA10_SS_1';
  l_property_name_src01  PROPERTYDEFS.NAME%type       := 'QA10_Simple2';
  l_field_group_name_src02 BUNDLEDEFS.NAME%type       := 'QA10_LargeText';
  l_property_name_src02  PROPERTYDEFS.NAME%type       := 'QA10_S3';
  l_field_group_name_src03 BUNDLEDEFS.NAME%type       := 'Core Attributes';
  l_property_name_src03  PROPERTYDEFS.NAME%type       := 'Resource Description';
  l_field_group_name_src04 BUNDLEDEFS.NAME%type       := 'MG_7';
  l_property_name_src04  PROPERTYDEFS.NAME%type       := 'MG_S7';
  l_field_group_name_src05 BUNDLEDEFS.NAME%type       := 'MG_4';
  l_property_name_src05  PROPERTYDEFS.NAME%type       := 'MG_S4';
  l_field_group_name_src06 BUNDLEDEFS.NAME%type       := 'MG_5';
  l_property_name_src06  PROPERTYDEFS.NAME%type       := 'MG_S5';
  l_field_group_name_src07 BUNDLEDEFS.NAME%type       := 'MG_6';
  l_property_name_src07  PROPERTYDEFS.NAME%type       := 'MG_S6';
  l_field_group_name_src08 BUNDLEDEFS.NAME%type       := 'MG_3';
  l_property_name_src08  PROPERTYDEFS.NAME%type       := 'MG_S3';
  l_separator           OP_GLOBALS.DB_Max_String_T   := ',';
  l_object_type_name    ASSETYPES.NAME%type         := 'SOXBusEntity';
  l_field_group_name    BUNDLEDEFS.NAME%type         := 'QA10_LargeText';
  l_property_name        PROPERTYDEFS.NAME%type      := 'TEST101';
  l_property_desc        PROPERTYDEFS.DESCRPTION%type := 'MGMGMGMGDescription';
  l_large_text_length    PROPERTYDEFS.DATA_LENGTH%type := '';
  OP_OBJ_MODEL_MGR.g_dl_longtext_medium;
  l_is_done_by_vendor    OP_Globals.Flag_String_T    := OP_Globals.sc_False;
  l_remote_address       i18n_audit_trail.remote_address%type := '';
  l_remote_host          i18n_audit_trail.remote_host%type   := '';
  l_preview_only         OP_Globals.Flag_String_T    := OP_Globals.sc_False;
  l_override_objtp_logic OP_Globals.Flag_String_T    := OP_Globals.sc_False;

```

Entity Move/Rename utility

The IBM OpenPages with Watson Entity Move/Rename utility allows batch processing of multiple Business Entities for overnight or weekend execution without running the risk of operations that time out. You can run the utility interactively or as a scheduled job.

Using the Entity Move/Rename utility, you can do the following:

- Rename a Business Entity hierarchy
- Simultaneously rename and move a Business Entity hierarchy

A single batch job can contain multiple independent operations, multiple dependent operations, or any combination thereof.

Each operation provides transactional consistency. If an operation fails, all the pending changes for this operation are rolled back. If an operation succeeds, all the changes are persisted.

Each rename, move, or combined operation runs in its own transactional context. So, failure in one operation does not result in the failure of the entire batch job.



CAUTION: Before running the utility, you must stop all application services to avoid data or security errors.

Entity Move/Rename utility prerequisites

Before you use the IBM OpenPages with Watson Entity Move/Rename utility, consider these prerequisites.

- A physical computer or VM that meets the OpenPages with Watson installation requirements. For detailed specifications, see the *IBM OpenPages with Watson Installation and Deployment Guide*.
- An application that produces either CSV (comma-separated value) files or Unicode tab delimited files. This application can be installed on any computer in your environment and is used to prepare the input data for the utility.
- User name and password for the Oracle or IBM Db2 account that owns the OpenPages application database schema (for example, OPENPAGES).

Configuring the Entity Move/Rename utility for an Oracle database

You must configure parameters in the OpenPages with Watson Entity Move/Rename utility before you use it in an Oracle database environment.

Procedure

1. Go to the Entity Move/Rename utility installation location as follows:
`OP_Home|aurora|bin|batch_entity_move_rename_relative`
2. Open the `batch-entity-move-rename.ini` configuration file for editing.
3. Specify appropriate values in the following parameters for an Oracle database environment:

Table 244. Parameters for an Oracle database in the <code>batch-entity-move-rename.ini</code> file:	
Parameter Name	Description
connect_string	Oracle database connection details. Use either the TNS alias or EZCONNECT format. TNS: <user>/<password>@<TNS alias> EZCONNECT: <user>/<password>@//<host>:<port>/<sid>

Table 244. Parameters for an Oracle database in the *batch-entity-move-rename.ini* file:
(continued)

Parameter Name	Description
data_format	Format of the input file to the utility. Example: csv or unicode-text Use the csv file format as follows: - Only if the data is known to contain ASCII characters exclusively. - All the national characters in the data input file are produced from the same Windows or ISO code page that is configured on the computer. You must specify the correct Oracle character set name that matches the code page in the character_set parameter.
input_file	Name of the input file (including extension). Example: 'Sample-batch-entity-move-rename.txt'
character_set	ANSI/ISO character set that is used by the utility. If the data_format parameter is set to csv, you must use a correct Oracle character set name that corresponds to the ANSI/ISO code page used by the OS (such as, WE8MSWIN1252). If the data_format parameter is set to unicode-text, this parameter is ignored.
skip_rows	The number of rows in the input files to skip on load. Example If the first row of the file: - Contains a list of column names, set the value to '1'. - Does not contain a list of column names, set this value to '0'.

4. Save and close the *batch-entity-move-rename.ini* configuration file.

5. Prepare the input file. See [“Prepare the input file for the Entity Move/Rename utility” on page 710](#).

Prepare the input file for the Entity Move/Rename utility

The input file for the Entity Move/Rename utility can be in CSV or Unicode tab delimited format. You can use any editor to create the input files. Included in the utility installation folder is a sample Unicode text file (.txt format).

Important: On Linux, the text input file must be saved or converted to be encoded in UCS-2 Little Endian and have Linux end of line (LF) characters.

Tip: If you are using Microsoft Excel, you must save the spreadsheet as a CSV or tab delimited file.

The input file must have the following five columns of data:

Table 245. Columns in the input file		
Column Name	Description	Sample Value
Source entity location	The entity on which the operation is run.	/The Bank/USA/North East/Providence

Table 245. Columns in the input file (continued)

Column Name	Description	Sample Value
Target entity location	The new parent entity for "move" and "move and rename" operations only. Note: - For Oracle "rename" operations only (no move), the value must be "-" (dash). - For Db2 "rename" operations only (no move), the value must be blank.	For "move" and "move and rename" operations: /Worldwide/ Americas/USA/NE
Run as user	Application user name, whose identity is used to run the operation.	OpenPagesAdministrator
New entity name	The new name after the operation for "rename" and "move and rename" operations only. Note: - For Oracle "move" operations only (no rename), the value must be "-" (dash). - For Db2 "move" operations only (no rename), the value must be blank.	For "rename" and "move and rename" operations: Boston
Execution order	Establishes the operation execution order as follows: - Operations that specify the execution order are run before operations that do not. - Operations that have a numeric value in the execution order column are run in regular ascending ordering. If set, the value must to be a valid number; Otherwise, leave the field blank.	1

The following is a short description of the data in the sample .txt file that is included in the utility directory.

- The first line illustrates moving entity /The Bank/USA/North East/Providence to new location /Worldwide/Americas/USA/NE. Operation is to be run as the user SOXAdministrator. This operation is run first in the batch.
- The second line illustrates in place rename of the entity /Worldwide/Americas/USA/NE/ Providence. Entity name changes to Boston. Target location does not apply and is set to "-". This entry has a dependency on the previous move operation and has higher number in the execution order column. Also, it references to the new entity location that will be in effect after the first operation completes.
- If the first operation fails for any reason, this operation fails as well and the entity location would be incorrect.
- The third line illustrates simultaneous move of the entity /The Bank/USA/Midwest/Chicago to new location /Worldwide/Americas/USA/MW and rename to Detroit. This operation has no dependencies and will be run after the first two complete.

If you have an Oracle database with the 32-bit SQL*Loader utility in a Linux environment, see the topic: [“Avoid error 0509-036 when you use the 32-bit Oracle SQL*Loader” on page 761](#). Otherwise, run the IBM OpenPages with Watson Entity Move/Rename utility.

Avoid error 0509-036 when you use the 32-bit Oracle SQL*Loader

This task applies only to the Entity Move/Rename operation if you use the 32-bit SQL*Loader utility with Oracle databases in Linux environments. Skip this task if you are using the 64-bit SQL*Loader utility.

If you use the 32-bit SQL*Loader (**sqlldr**) utility, the following system error might be displayed:

```
exec(): 0509-036 Cannot load program sqlldr because of the following errors:
      0509-026 System error: There is not enough memory available now.
Failure while executing the Oracle SQL*Loader. Exit code is 255
```

If the 0509-036 system error is displayed, you can set the Loader Control environment variable by opening a shell window and running the following command:

```
export LDR_CNTRL=MAXDATA=0x80000000 at LARGE_PAGE_DATA=Y
```

Tip: If you are running the IBM OpenPages with Watson Entity Move/Rename utility as a scheduled **cron** job, make sure to set the Loader Control environment variable in the **cron** environment.

When finished, run the IBM OpenPages Entity Move/Rename utility. See [“Running the entity move/rename utility interactively” on page 761](#) or [“Running the Entity Move/Rename utility as a scheduled task” on page 712](#).

Running the entity SQL*move/rename utility interactively

Use the following steps to run the IBM OpenPages with Watson Entity Move/Rename utility interactively in an Oracle database environment.

Before you begin, make sure that you prepared the input file. See [“Prepare the input file for the Entity Move/Rename utility” on page 710](#) for instructions.

Procedure

1. Move the input file into the utility installation directory, which is at:

```
OP_Home|aurora|bin|batch_entity_move_rename_relative
```

2. Validate that the **input_file** parameter in the `batch-entity-move-rename.ini` configuration file is correctly set to the input file name. For more information, see [“Configuring the Entity Move/Rename utility for an Oracle database” on page 758](#).
3. From the location where the utility is installed, run the batch command file and review the output on the screen.

Windows

batch-entity-move-rename.cmd

Linux

batch-entity-move-rename.sh

4. Upon completion, review the following log files for any errors:
 - `batch-entity-move-rename-load.log`
 - `batch-entity-move-rename-proc.log`

If any errors are reported and you are unable to fix them, contact IBM OpenPages Support. Make sure you supply a copy of the screen that contains the error messages and all the log files that are generated by the tool.

Running the Entity Move/Rename utility as a scheduled task

You can set up a scheduled task to run the IBM OpenPages with Watson Entity Move/Rename utility.

Depending on your environment, you can run the `batch-entity-move-rename` batch command file by using any scheduling application. For example, in Windows, you might use the built-in Windows scheduler. In Linux, you might set up a **cron** job.

Important: If you are using a Db2 database in a Windows environment, you must run the batch command file within the **Db2 Command Line Processor**.

If the job fails, the batch command returns a non-zero exit code. You can redirect the console output to a log file. For example, in Windows:

```
batch-entity-move-rename.cmd >> batch-entity-move-rename.log
```

The following files are overwritten on each run:

- `batch-entity-move-rename-load.log`
- `batch-entity-move-rename-proc.log`

These files can be saved, either manually or through a script, if log archives are needed.

Impact of the Entity Move/Rename utility on the OpenPages application

The Entity Move/Rename utility works directly against the IBM OpenPages with Watson database repository. As a result, the Java based OpenPages application is unaware of the changes made to the entity hierarchy and folder structure.

As a result, internal application caches might become out of sync with the data in the repository and lead to discrepancies in the application user interface.

It is required that after you run the tool you restart application services, or run the tool when application services are stopped.

Also, ensure that the **OPBackup** command is not running during execution, and that all batch rename and move operations are completed before you run a backup.

Chapter 23. System Maintenance

You can perform system maintenance tasks such as changing the default port numbers, changing password references, and so on.

Application server restrictions

When you are performing system maintenance, be aware of the restrictions for IBM OpenPages with Watson application servers.

- Do not rename application servers. The OpenPages property files contain hard-coded references to the application servers.

Port assignments

Both dedicated ports and ports that are dynamically assigned for each installation are used for the IBM OpenPages with Watson installation. These default ports can be changed after installation.

Default ports

The following table lists the default ports.

Table 246. Default fixed port assignments	
Description	Ports
OpenPages installation server	8443
OpenPages installation agent	8443
OpenPages database instance (Oracle)	1521
OpenPages database instance (IBM Db2)	50000
OpenPages application URL	10108
OpenPages application URL (SSL)	10111
Cognos Analytics gateway (as configured for your web server)	80
Framework Generator port	8080
Cognos Analytics dispatcher URI	9300
Search server (used for indexing and searching OpenPages data)	8983
Search server (used to administer global search)	8985

Files containing port numbers

After installation, you can view the OpenPages application port assignments in the following file on each application server: `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties`.

The following tables list property files on the OpenPages admin application server that contain port numbers for other components.

Table 247. Files that contain port numbers		
Port	File name	Parameter Name
Application server ports	<OP_HOME>/wlp-user/servers/ <server_name>Server<#>/ bootstrap.properties	op.http.port op.https.port if you are using SSL
Oracle database instance port	<ORACLE_HOME>/NETWORK/ ADMIN/tnsnames.ora	N/A
Framework Generator port	<OP_HOME>/aurora/conf/ aurora.properties	cognos.framework.refresh. servlet
Cognos Analytics server port	<OP_HOME>/aurora/conf/ aurora.properties	cognos.server
Cognos Analytics Dispatcher URI	<OP_HOME>/aurora/conf/ aurora.properties	cognos.computation. server

Dynamically assigned ports

Port numbers for IBM OpenPages with Watson servers that are not listed, are assigned dynamically during the installation.

For application servers, when you add a horizontal cluster member, you specify a port number on the application server card in the installation app. The next 20 port numbers are reserved for each vertical cluster member.

Change default port numbers

You can change the default IBM OpenPages with Watson port numbers after installation.

Important: Only ports 80, 443, or an open port in the range 1024 - 65535 can be used as the IBM OpenPages with Watson application port number.

The OpenPages with Watson installer sets several default ports during installation, such as the ports for the OpenPages server.

After installing the application, you can change the OpenPages ports to different ports, if needed. For example, in the event of a port conflict, where another application is using these port ranges, you can change the OpenPages ports to avoid the conflict.

For a port conflict, change all of the OpenPages application server ports to a new range. Follow the instructions in the following section.

Important:

- Do not change the port number for the OpenPages with Watson administrative server.
- To modify port numbers on other application servers in a cluster, repeat the following tasks on each cluster member.

Checking port number availability

Before changing the port numbers, make sure that the new ports you are going to use are available.

To determine if another application is using a specific port, log onto the application server where you need to change the port. Open a command or shell window and execute the following command:

Windows

```
netstat -an | findstr <port number>
```

Linux

```
netstat -an | grep <port_number>
```

Changing OpenPages with Watson application ports for an WebSphere Liberty environment

Because the IBM OpenPages with Watson application on IBM WebSphere Liberty uses port ranges, if you need to change one of the OpenPages environment port numbers, you should change all of the OpenPages application server ports to a new range.

By default, the OpenPages with Watson application on WebSphere Liberty uses the port range 10101-10120.

Updating the port numbers in WebSphere

Use the following steps to change the default port numbers of an IBM OpenPages with Watson application server.

Procedure

1. Log on to the application server.
2. Stop the application servers.
For more information, see [“Stopping application servers” on page 843](#).
3. Open the following file in a text editor: `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties`
Where `<server_name>` is the name of the application server.
4. Update the application port number.
 - If you are using TLS, update the `op.https.port` value.
 - If you are not using TLS, update the `op.http.port` value.
5. Save your changes.
6. Repeat these steps on each horizontal application server.
7. Restart the application servers.
For more information, see [“Starting application servers” on page 841](#).

What to do next

If you changed the OpenPages application port or the secure application port, you must manually change the port values in the following properties files for the OpenPages application server for which you changed the ports:

- `<OP_HOME>/aurora/conf/aurora.properties`
- `Server<#>-sosa.properties`
- `Server<#>-server.properties`

Updating the Java Messaging ports on the OpenPages with Watson server

You can change the ports that are used by the Java Messaging Service.

About this task

WebSphere Liberty uses the Java Message Service (JMS) to enable Java clients and applications to create, send, receive, and read asynchronous requests.

Procedure

1. Log on to the application server.
2. Stop the application servers.
For more information, see [“Stopping application servers” on page 843](#).
3. Open the following file in a text editor: `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties`
Where `<server_name>` is the name of the application server.
4. Update the application port number.
 - If you are using TLS, update the `op.jmss.port` value.
 - If you are not using TLS, update the `op.jms.port` value.
5. Save your changes.
6. Repeat these steps on each horizontal application server.
7. Restart the application servers.
For more information, see [“Starting application servers” on page 841](#).

Updating the application port values in the server and tools client properties files

If you changed the IBM OpenPages with Watson OpenPages application port (10108 or 10111, for example), you must manually change the port values in the server and tools client properties files.

Procedure

1. Log on to each IBM OpenPages with Watson application server as a user with administrative privileges.
2. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
3. Go to the `<OP_HOME>/aurora/conf` directory.
4. Open the `Server<#>-server.properties` file in a text editor.
5. If you changed the application port, edit the following lines to update the port numbers.

```
url.path.openpages=http\://<server>:<port>/openpages  
webclient.http.server.port=<port>
```

6. Save and close the file.
7. Go to the `<OP_HOME>/bin` directory.
8. Open the `openpages-tools-client.properties` file in a text editor.
9. If you changed the application port, update the `rest.url.path` property with the new port number.
For more information, see [“Tools properties and parameters” on page 1085](#).
For example:

```
rest.url.path=https\://localhost:10111/grc/api
```

10. Save and close the file.
11. Restart all OpenPages application servers.
For more information, see [Chapter 24, “Starting and stopping servers,” on page 841](#).

Updating port values in the `aurora.properties` file

You can update port values in the `aurora.properties` file.

Procedure

1. Log on to the IBM OpenPages with Watson admin server associated with the application server for which you changed ports as a user with administrator privileges.
2. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
3. Go to the `<OP_HOME>/aurora/conf` directory where `<OP_HOME>` represents the installation location of the OpenPages application.
4. Locate the `aurora.properties` file in the `conf` directory and open the file in a text editor.
5. If you changed the OpenPages application port number (10108 or 10111 by default), update the port in the following property:

```
application.url.path=
```

Updating port values in the database

If you updated any of the default IBM OpenPages with Watson ports, you must update the port value(s) in the `REGISTRY_ENTRIES` table in the IBM OpenPages database as follows.

Procedure

1. Log on to a machine with SQL*Plus and access to the database server.
2. Run the following SQL commands to update the port number in the `REGISTRY_ENTRIES` table:

```
update registryentries set value='<new_port_number>'
where path='/OpenPages/Platform/Reporting Schema/Object URL Generator/Port';
commit;
```

where `<new_port_number>` is the new OpenPages application server port number.
3. When the commands are complete, log out of SQL*Plus.

Updating port values on the reporting server

If you changed the IBM OpenPages with Watson application port number, you must update the associated CommandCenter instance with the new port number.

Procedure

1. Log onto the reporting server as a user with administrator privileges.
2. Open an Linux shell and navigate to the `<Cognos_Home>/configuration` directory where `<Cognos_Home>` represents the installation location of the Cognos application.
3. Locate the `OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties` file and make a backup copy of the file.
4. Open the `OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties` file in a text editor of your choice and do the following:
 - a) Replace the existing OpenPages with Watson application port number (10108) update the following property with the new OpenPages application port number:

```
openpages.application.url=
```

- b) Save and close the file.

Changing the OpenPages with Watson Framework Generation port

You can change the port number that the IBM OpenPages with Watson Framework Model Generator Service runs on.

Procedure

1. Log on to the IBM Cognos Reporting Server as the owner of the OpenPages CommandCenter installation.
2. Stop the OpenPages Framework Model Generator Service.

Windows:

Right-click the IBMOpenPagesFrameworkModelGenerator service and select **Stop**.

Linux:

- a. Open a shell as a user with administrative privileges and navigate to the following directory:

```
<CommandCenter_Home>/wlp/bin
```

Where *<CommandCenter_Home>* is the installation location of OpenPages with Watson CommandCenter. By default, this location is: /opt/OpenPages/CommandCenter.

- b. Run the following command:

```
server stop IBMOpenPagesFrameworkModelGenerator
```

3. In the `server.xml` file, update the HTTP and HTTPS port and allow a connection to the host from the remote system. For example:

```
<op_home>\CommandCenter\wlp\usr\servers\defaultServer
```

4. In the `server.xml` file, search for the following block of text:

```
<!-- A "Connector" represents an endpoint by which requests are received
and responses are returned. Documentation at :
Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
Java AJP Connector: /docs/config/ajp.html
APR (HTTP/AJP) Connector: /docs/apr.html
Define a non-SSL HTTP/1.1 Connector on port 8080
-->
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" />
```

5. Change `port="8080"` to the port number you want the services to run on.
6. Start the OpenPages Framework Model Generator Service.

Windows:

Right-click the IBMOpenPagesFrameworkModelGenerator service and select **Start**.

Linux:

- a. Open a shell as a user with administrative privileges and navigate to the following directory:

```
<CommandCenter_Home>/wlp/bin
```

Where *<CommandCenter_Home>* is the installation location of OpenPages with Watson CommandCenter. By default, this location is: /opt/OpenPages/CommandCenter.

- b. Run the following command:

```
server start IBMOpenPagesFrameworkModelGenerator
```

7. Log on to the OpenPages server as the OS owner of the OpenPages software and stop the services by using `stopAllServers`.

8. Go to <OPENPAGES_HOME>\aurora\conf, where <OPENPAGES_HOME> is the installation location of the OpenPages software. Typically, the location is C:\OpenPages for Microsoft Windows servers and /opt/OpenPages for Linux systems.
9. In the `aurora.properties` file, change the port number for the following entry to the value that you set it to in step 5:

```
cognos.framework.refresh.servlet=http\://reporting-server\:8080/crf-refresher/
```

In this case, you would change 8080 to the new port number.

10. Restart the OpenPages services.
11. Log on to OpenPages as the OpenPagesAdministrator.
12. Update the reporting schema and framework. For more information, see [“Creating or recreating the reporting schema \(Standard UI\)” on page 163](#).

What to do next

- Application server names - After OpenPages is installed, the application server name cannot be changed. Many configuration files, such as **aurora.properties**, include the application server names as an embedded string. The name cannot be changed after installation.
- Restart services - After you complete the port changes, restart OpenPages. For details, see [Chapter 24, “Starting and stopping servers,” on page 841](#).
- Update the reporting schema and Framework - After services are restarted, you must re-create the reporting schema and regenerate the Reporting Framework. Doing so allows the port change to be reflected in any redirects of reports. For more information, see [“Creating or recreating the reporting schema \(Standard UI\)” on page 163](#).

Updating URL host pointers for reports

After you migrate, change port settings in a production environment, or if you want to refresh a test environment from a production database, you might need to update the URL host pointers on the application server so that links in reports work properly.

You need to update the URL host pointers if the host, port, or protocol of the application server has changed. Check the **Object Generator URL** setting to verify that the host, port, and protocol are correct. If the port, host, and protocol are correct, you do not need to do this task.

You can update links in reports by modifying URL host pointer settings, and then propagating these reporting schema changes to the application server.

To update the reporting schema, you can do either of the following:

- Run an SQL script that incrementally updates the reporting schema with the changes (recommended).
Note: For SQL tool information, see the topic "Database tool information" in the *IBM OpenPages with Watson Administrator's Guide*.
- Use the IBM OpenPages with Watson application user interface to re-create the entire reporting schema.

Procedure

1. Start the IBM OpenPages with Watson services on the admin application server.
2. Log on to the OpenPages with Watson application user interface as a user with administrator privileges.
3. Open the **Settings** page.
 - In the Task Focused UI, click  > **System Configuration** > **Settings**.
 - In the Standard UI, click **Administration** > **Settings**.

To access settings, you must have the **Settings** application permission set on your account.

4. Change the **Object URL Generator** settings.

- a) Expand **Platform > Reporting Schema > Object URL Generator**.
- b) Update the **Object Generator URL** settings, as required, to point to the application server (such as a test application server). Make sure to click **Save** after you modify each setting.

Table 248. Object Generator URL settings

Setting Name	Description
Host	The changed name of the application server. Example : test-eng1
Port	The changed port number of the application server. Example : 10108
Protocol	The changed protocol for accessing the application server. Valid values are either http or https.

5. To update the changed URL setting on the application server, update the reporting schema using one of the following methods:

- Method 1: Run the following SQL script to incrementally update the reporting schema (recommended):
 - a. From a computer with a SQL tool and access to the database server, log on to SQL as the OpenPages database user (for example, openpages).
 - b. Run the following SQL statements to update the reporting schema:

```
begin
OP_RPS_MGR.SET_DETAIL_PAGE_URL_IN_RPS_RT;
end;
/
```

- Method 2: Re-create the entire reporting schema by using the application user interface. For more information, see "Creating or recreating the reporting schema" in the *IBM OpenPages with Watson Administrator's Guide*.

Auditing configuration changes

The IBM OpenPages with Watson provides you with the capability of tracking configuration changes made to your system through the Configuration Audit Report.

Accessing the Configuration Audit Report

To view and generate the Configuration Audit Report, you must have the reporting schema and framework enabled and configured on your system.

Procedure

1. In the menu bar, click **Analytics**. Click **Team Reports**, and then click **OpenPages Platform V6 > Audit Reports > Configuration**.
Or, in the Standard UI, click **Reporting** and do one of the following steps:
 - Select **OpenPages V6 > Audit Reports > Configuration**.
 - Click **All Reports**, and navigate to the **OpenPages V6** folder (if necessary, click the plus sign to expand the folder tree). In the folder tree, expand **Audit Reports > Configuration**.

Important: In reference to Reporting Framework V6, V6 refers to the latest framework version, not to any specific OpenPages release number.

2. Click **Configuration Audit** to run the report.
3. On the **Configuration Audit Report** page, specify the date range for the reporting data as follows:
 - a) Type a start date or click the calendar arrow and select a start date.
 - b) Type an end date or click the calendar arrow and select an end date.
 - c) Click **Finish** to generate the report.

The Configuration Audit Report

The Configuration Audit Report tracks any metadata changes made to field groups, object types, application text, object text, profiles, settings, and views and dashboards in the Task Focused UI.

- Field Groups - such as modifications made to object field definitions and enumerated string values.
- Object Types - such as the inclusion of Field Groups and changes in parent and/or child object relationship rules (for example, cardinality setting changes or enabling/ disabling object type relationships).
- Application Text or Object Text - such as translation changes to locale-specific display labels for object types, object fields, and enumerated string values. You can enable or disable the auditing of translated text. By default, auditing is enabled.
- Profiles - such as modifying object views and showing or hiding object types and fields.
- Registry settings.
- Views that are defined in the Task Focused UI.
- Dashboards that are defined in the Task Focused UI.

Table 249 on page 771 describes the various audited configuration changes contained in the report under the following column headings:

<i>Table 249. Audit Configuration Column Headings</i>	
This report column...	Contains this type of data...
Object	The type of object that was modified.
Category	A category or classification under the object type.
Action Type	The type of action performed on the object.
Action Date	The date the action was performed.
Created by	The name of the user who performed the action.
Old Value	The value before it was modified.
New Value	The value after it was modified.

Changing the password of the WebSphere Liberty keystore

You can change the password of the IBM WebSphere Liberty keystore.

Procedure

1. Log on to the OpenPages admin application server.
2. Open a command or shell window.

3. Run the following command:

```
keytool -storepasswd -keystore <OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/  
security/key.p12 -storetype PKCS12 -storepass <current_password>
```

Replace *<current_password>* with the current password of the keystore. The initial password of the keystore is the same as the OpenPagesAdministrator password that you set when you installed OpenPages.

4. Follow the prompts to set the new password.
5. Encrypt the password by running the following command:

```
<WLP_HOME>/bin/securityUtility.sh|.bat encode --encoding=aes <new_password>
```

Replace *<new_password>* with the password that you created in step 4.

The script returns the encrypted password.

6. Update the `bootstrap.properties` file with the new encrypted password.
 - a) Open the following file in a text editor: `<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/bootstrap.properties`
 - b) Update the value of the `keystore.password` parameter with the encrypted password from step 5.
 - c) Save and close the file.
7. Restart all application services.

For more information, see [“Starting application servers” on page 841](#).
8. Repeat these steps on each horizontal cluster application server.

Changing the keystore that is used by WebSphere Liberty

When you install IBM OpenPages with Watson, the installation process configures a keystore for IBM WebSphere Liberty. If you have an existing keystore or if you want to use an alternate keystore, you can change the keystore that is used by WebSphere Liberty. This task is optional.

Procedure

1. Log on to the application server.
2. Encrypt the password of the keystore that you want to use for WebSphere Liberty.

Run the following command:

```
<WLP_HOME>/bin/securityUtility.sh|.bat encode --encoding=aes <keystore_password>
```

Replace *<keystore_password>* with the password of the keystore.

The script returns the encrypted password.

3. Edit the following file:
`<OP_HOME>/wlp-usr/servers/<server_name>/configDropins/overrides/op-apps.xml`
4. Update the following line to point to the keystore that you want to use.

```
<keyStore id="defaultKeyStore" location="<keystore_file>" password="<encrypted_password>" />
```

Replace *<keystore_file>* with the path and filename of the keystore. Replace *<encrypted_password>* with the encrypted password from step 2.

For example:

```
<keyStore id="MyKeyStore" location="/home/opuser/OP/OpenPages/wlp-usr/servers/opappServer1/  
resources/security/my_keystore.p12" password="<encrypted_password>" />
```

5. Restart all application services.

For more information, see [“Starting application servers” on page 841](#).

6. Repeat these steps on each horizontal cluster application server.

Changing the keystore that is used by Db2

When you install IBM OpenPages with Watson, the installation process configures a keystore for IBM WebSphere Liberty. By default, the Liberty keystore is also used for Db2. If you have an existing keystore or if you want to use an alternate keystore, you can change the keystore that is used by Db2. This task is optional.

Procedure

1. Log on to the application server.
2. Locate the keystore that you want to use for Db2 and copy it to the following directory on the application server: `<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/`
3. Copy the `<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/op-db2.xml` file to the following directory: `<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/configDropins/overrides/`.

Do not modify or delete the `<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/op-db2.xml` file.

4. Open the following file in a text editor: `<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/configDropins/overrides/op-db2.xml`
5. Locate the following line:

```
<properties.db2.jcc databaseName="<op_db_name> portNumber="<op_db.port>"
  serverName="<op_db.host>" user="<op_jdbc_user>" password="<op_jdbc_password>"
  enableExtendedDescribe="2" />
```

6. Add the following attribute to the `properties.db2.jcc` element:

```
sslConnection="true" sslTrustStoreLocation="<db_keystore_file>"
sslTrustStorePassword="<db_keystore_password>" sslTrustStoreType="PKCS12"
```

Replace `<db_keystore_file>` with the path and filename of the keystore. Replace `<db_keystore_password>` with the encrypted password of the keystore.

For example:

```
<properties.db2.jcc databaseName="OPX" portNumber="50001" serverName="db.host.com" user="op"
  password="password" enableExtendedDescribe="2" sslConnection="true"
  sslTrustStoreLocation="/home/opuser/OP/OpenPages/wlp-usr/servers/opappServer1/
  resources/security/db.p12" sslTrustStorePassword="password" sslTrustStoreType="PKCS12" />
```

7. Restart all application services.
For more information, see [“Starting application servers” on page 841](#).
8. Repeat these steps on each horizontal cluster application server.

Changing the OPSystem password

You can change the password of the OPSystem account. OPSystem is a default service user account that is required by internal system actions.

Procedure

1. Start all services.
2. Open a command or shell window on the application server.
3. Navigate to the `<OP_Home>|bin` directory.

For Microsoft Windows operating systems, the default installation directory of OpenPages with Watson is C:\OpenPages.

For Linux operating systems, the default installation directory of OpenPages with Watson is /opt/OpenPages.

Tip: You can also run the chng-sys-pswd tool from a remote system, such as your laptop. For more information, see [“Installing tools and utilities \(IBM OpenPages with Watson\)” on page 824](#)

4. Run one of the following commands to open the chng-sys-pswd tool:

Windows

```
chng-sys-pswd.bat
```

Linux

```
chng-sys-pswd.sh
```

You are prompted for the old OPSys password, and then the new password.

5. Follow the on-screen prompts.
6. When directed, stop all services.
7. Restart all services to enable the new password.

Changing database password references

If the password of the OpenPages database changes, you need to update password references with the new password.

Before you begin

Before you change password references for data sources in IBM OpenPages with Watson, make sure that you have the following:

- Administrative access to the following machines and application:
 - OpenPages application server
 - Cognos Analytics server
 - IBM Cognos Analytics application
- The current and new password for the following database users:
 - OpenPages database user

About this task

To change database password references, you must do the following tasks:

- [“Change database password references on the OpenPages with Watson application server” on page 775](#)
- [“Modifying the OpenPages database password in Cognos ” on page 776](#)
- [“Modifying database passwords in the backup-restore environment files \(Oracle only\)” on page 776](#)

If you need information about encrypting database passwords in the backup and restore utility environment files, see [“Encrypting database passwords in the backup-restore utility environment files” on page 717](#).

- If you use global search, update the login information for the search server. See [“Changing the login information for the search server” on page 652](#)

Change database password references on the OpenPages with Watson application server

The process for changing the database password on the IBM OpenPages with Watson application server requires two tasks.

[“Modifying the JDBC data source password” on page 775](#)

[“Updating the application server database password in the aurora.properties file” on page 775](#)

Important: Make a backup copy of each file before modifying it.

Modifying the JDBC data source password

If the JDBC data source password changes, you need to update the bootstrap.properties file on each application server.

Procedure

1. Log on to the OpenPages application server.
2. Open a command or shell window.
3. Encrypt the password by running the following command:

```
<WLP_HOME>/bin/securityUtility.sh|.bat encode --encoding=aes <new_jdbc_password>
```

Replace <new_jdbc_password> with the database password.

The script returns the encrypted password. Copy the password.

4. Update the bootstrap.properties file with the new encrypted password.
 - a) Open the following file in a text editor: <OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties
 - b) Update the value of the op.jdbc.password parameter with the encrypted password from step 3.
 - c) Save and close the file.
5. Restart all application services.

For more information, see [“Starting application servers” on page 841](#).
6. Repeat these steps on each horizontal cluster application server.

Updating the application server database password in the aurora.properties file

To change the database password on the IBM OpenPages with Watson application servers, one task that you must do is to edit the aurora.properties file.

Note: This information applies to Windows and Linux environments.

Procedure

1. Open a command or shell window and navigate to the <OP_Home>|aurora|conf directory.

Table 250. Installation location of the OpenPages with Watson application	
Operating system	Installation location
Windows	For example, <OP_Home> C:\IBM\OpenPages
Linux	For example, <OP_Home> /opt/IBM/OpenPages

2. Locate the aurora.properties file in the conf directory and do the following:
 - a) Make a backup copy of the file before modifying it.

- b) Open the file in a text editor of your choice.
- c) Search the file for the string database .PASSWORD.
- d) Change the value following the equal sign to the new password.
- e) Save your changes and exit the editor.

Note: The password becomes encrypted when the services are restarted.

3. Repeat these steps on each application server.

Modifying the OpenPages database password in Cognos

If you change the IBM OpenPages with Watson database password, you must update the OpenPages DataSource in IBM Cognos Analytics. If you have an Oracle database environment, you must also update the Oracle Native Driver.

Procedure

1. Ensure that all application servers and reporting servers are running.
2. Open a browser window and log on to the OpenPages with Watson application user interface as a user with administrative permissions.
3. From the navigation bar, select **Reporting > Cognos Analytics**.
4. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
5. Click the **Configuration** tab.
6. Click the link for the **OpenPages DataSource**, and then click **OpenPages DataSource**.
The **Directory > Cognos > OpenPages DataSource > OpenPages DataSource** page is displayed.
7. Under the **Actions** column, click the **Set properties - OpenPages DataSource** icon .
8. Click the **Signon** tab.
9. Click the **Edit the signon** link.
10. Type the password of the OpenPages database, and then click **OK**.
11. If you use Oracle, do the following additional steps:
 - a) Return to the **Directory > Cognos** page.
 - b) Click the link for the **Oracle Native Driver**, and then click **Oracle Native Driver**.
The **Directory > Cognos > Oracle Native Driver > Oracle Native Driver** page is displayed.
 - c) Click the **Signon** tab.
 - d) Click the **Edit the signon** link.
 - e) Type the password of the OpenPages database, and then click **OK**.
12. Log out of OpenPages.
13. Restart all OpenPages application servers.
14. Log on to OpenPages and open a report to test Cognos.

Modifying database passwords in the backup-restore environment files (Oracle only)

If you change the IBM OpenPages database password, you need to update the environment files that are used by the backup and restore utilities.

This task applies only to Oracle database environments.

Procedure

1. Repeat these steps on each application server.
2. Open a command or shell window as an administrator.

3. Go to the `<OP_Home>/aurora/bin` directory and locate the `op-backup-restore.env` file.
 4. Make a backup copy of the `op-backup-restore.env` file.
 5. Open the `op-backup-restore.env` file in a text editor.
 6. Update the following passwords:
 - `DB_SYSTEM_PWD`: Type the password of the SYSTEM user for the OpenPages database.
 - `DB_SYS_PWD`: Type the password of the DBA user for the OpenPages database.
 - `DB_OP_PWD`: Type the password of the schema owner for the OpenPages database.
 7. Go to the `<CC_Home>/tools/bin` directory and locate the `op-cc-backup-restore.env` file.
 8. Make a backup copy of the `op-cc-backup-restore.env` file.
 9. Open the `op-cc-backup-restore.env` file in a text editor.
 10. Update the following passwords:
 - `DB_CC_PWD`: Type the password of the schema owner for the Cognos database.
- Note:** If you use the same database for OpenPages and the Cognos content store, enter the passwords for the OpenPages database DBA and schema owner.
11. Re-encrypt the passwords in the `op-backup-restore.env` and `op-cc-backup-restore.env` files.
See [“Encrypting database passwords in the backup-restore utility environment files”](#) on page 717.
12. Repeat these steps on each application server.

Updating the Oracle Enterprise Manager tool

If either the static IP address of the database server changes or the database host name changes, then the web-based Oracle Enterprise Manager tool (`https://<server_name>:<port>/em`), which is used for managing the Oracle database, will no longer function properly and requires reconfiguration.

Note: The Oracle database server requires a static IP address.

Resolving configuration changes in the tool

To resolve configuration changes so the Oracle Enterprise Manager Database Control tool functions properly, you must first deconfigure and then reconfigure the tool as follows.

Procedure

1. Open a command or shell window.
2. Change directory to `<ORACLE_HOME>/bin` as follows:

Windows

```
cd %ORACLE_HOME%\bin
```

Linux

```
cd $ORACLE_HOME/bin
```

3. Type the following command to deconfigure the Oracle Enterprise Manager tool:

```
emca -deconfig dbcontrol db -repos drop
```

4. Type the following command to reconfigure the Oracle Enterprise Manager tool:

```
emca -config dbcontrol db -repos create
```

Changing database references

If the database name (IBM Db2) or identifier (Oracle) changes, you need to update references to the database.

For example, if you have upgraded from an old database server to a new one, migrated from a non-RAC to a RAC environment, or are moving from a shared database environment to a stand-alone environment, then you must change several references on the IBM OpenPages with Watson application and reporting servers to point to the new database instance.

Note:

If you changed the database server host name, see the following topics:

- If you are using IBM Db2, see [How to Change the Hostname of an IBM DB2 Database Server for OpenPages](#).
- If you are using Oracle, see [How to Change the Hostname of an Oracle Database Server for OpenPages](#).

To change database references, you must take the following actions:

- If you are using IBM Db2, recreate the catalog entry for the OpenPages database, and then test the connection. You can see examples of the syntax in the following technote: [How to Change the Hostname of an IBM DB2 Database Server for OpenPages](#).
- If you are using Oracle, see “Testing the connection to the OpenPages database from the Oracle database client” on page 778
- “Modifying the data source connection URL” on page 779
- “Modify database references in the application configuration files” on page 779
- “Modify database connection references for the reporting server” on page 781

Before you begin

Make sure that you have the following information:

- Administrative access to the following machines and application:
 - OpenPages application server
 - OpenPages Cognos server
 - IBM Cognos Analytics application
 - OpenPages system account user and password
- For Oracle database environments, the Oracle System Identifier (SID) of the new database instance.
- For IBM Db2 database environments, the database name.

Testing the connection to the OpenPages database from the Oracle database client

Test whether the SQL*Net connect string can connect to the IBM OpenPages with Watson database on the Oracle database server from the Oracle database client.

Procedure

1. Copy the file `<ORACLE_HOME>/network/admin/tnsnames.ora` from the Oracle database server operating system to the `<ORACLE_HOME>/network/admin` Oracle database client directory on the application server or reporting server.

Ensure that the OpenPages installation user has read, write and execute permissions on the `tnsnames.ora` file in the Oracle database client operating system.

2. Log on to the application server or reporting server as an OpenPages installation user.

3. Edit the file `<ORACLE_HOME>/network/admin/tnsnames.ora`, and update the Host value to the host name or IP address of the Oracle database server.
4. To test the connection to the OpenPages database on the database server, type the following command:

```
sqlplus <username>/\"<password>\"@<service_name>
```

For example, `sqlplus system/\"password\"@op`

The system connects you to an Oracle database instance.

5. To exit SQL*Plus, type `exit`.

Modifying the data source connection URL

You can modify the JDBC data source in IBM WebSphere Liberty for the application server.

Procedure

1. Log on to the OpenPages application server.
2. Open the following file in a text editor: `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties`
3. Update the properties.

Db2

Set `op.jdbc.host` to the hostname of the database server.

Set `op.db2.portNumber` to the database port number.

Set `op.db2.databaseName` to the name of the Db2 database.

Oracle

Set `op.jdbc.host` to the hostname of the database server.

Set `op.ora.portNumber` to the database port number.

Set `op.ora.databaseName` to the Oracle System Identifier.

4. Save the file.
5. Restart all application services.
For more information, see [“Starting application servers” on page 841](#).
6. Repeat these steps on each horizontal cluster application server.

Modify database references in the application configuration files

Use the following instructions to update database references in the `aurora.properties` file. If you are using Oracle, you also need to update the `op-backup-restore.env` file.

Note: This information applies to Windows and Linux environments.

Modify the database reference in the `aurora.properties` file

You can update the database references in the `aurora.properties` file.

Procedure

1. Open a command or shell window and go to the `<OP_HOME>/aurora/conf` directory.
2. Locate the `aurora.properties` file in the `conf` directory and do the following tasks:
 - a) Make a backup copy of the file before you modify it.
 - b) Open the file in a text editor of your choice.
 - c) Search the file for the string `'database.URL'`.

d) Change the value that follows the equal sign to the new database connection URL.

- For Oracle database environments, the URL format might look similar to the following example.

```
database.URL=jdbc\:oracle\:thin:@//<host-name>\:<port>/<SID>
```

Where:

- *host-name* is the name of the database server, such as eng11.
- *port* is the database port number, such as 1521.
- *SID* is the Oracle System Identifier, such as OP.

- For IBM Db2 environments, the URL format might look similar to the following example.

```
database.URL=jdbc\:db2\://<host-name>\:<port>/<DATABASE_NAME>
```

Where:

- *host-name* is the name of the database server, such as eng11.
- *port* is the database port number, such as 50000.
- *DATABASE_NAME* is the name of the Db2 database, such as OP.

e) Save your changes and exit the editor.

3. Repeat these steps on each application server.

What to do next

If you are using Oracle, update the `op-backup-restore.env` file. For more information, see [“Modify database references in the OpenPages backup and restore environment file \(Oracle only\)” on page 780](#).

Modify database references in the OpenPages backup and restore environment file (Oracle only)

This task applies only to Oracle database environments. You must modify Oracle database references in the `op-backup-restore.env` file.

Procedure

1. Open a command or shell window and navigate to the `<OP_HOME>/aurora/bin` directory.

For information about `<OP_HOME>`, see [“Installation locations for IBM OpenPages with Watson” on page xxxiii](#).

2. Locate the `op-backup-restore.env` file in the `bin` directory and do the following:

- a) Make a backup copy of the file before modifying it.
- b) Open the file in a text editor of your choice.
- c) Search the file for the following strings:
 - `DATABASE_URL=jdbc\:oracle\:thin:@//<host-name>\:<port>/<SID>`
 - `DB_SID=<SID>`
 - `DB_ALIAS=<database_alias>`

Where:

- *<host-name>* is the name of the database server, such as eng11.
- *<port>* is the database port number, such as 1521.
- *<SID>* is the system ID of the database, such as OP.
- *<database_alias>* is the alias of the database, such as OP.

d) Change the value following the equal sign to the new database connection URL and SID.

- e) Save your changes and exit the editor.
3. Restart the OpenPages application servers.
4. Repeat these steps on each application server.

Modify database connection references for the reporting server

Use the following instructions to update database references in IBM Cognos Analytics. If you have an Oracle database environment, you must also update the `op-cc-backup-restore.env` file.

Note: This information applies to Windows and Linux environments.

Once the values are updated, you need to restart all reporting servers.

Modifying database connection references in Cognos

You must change the database connection reference values in IBM Cognos Analytics for the OpenPages DataSource. If you have an Oracle database environment, you must also update the Oracle Native Driver.

Procedure

1. Ensure that both the IBM OpenPages with Watson and IBM Cognos servers are running.
2. Open a browser window and log on to the OpenPages with Watson application user interface as a user with administrative permissions.
3. From the navigation bar, select **Reporting > Cognos Analytics**.
4. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
5. In the **IBM Cognos Administration** window, click the **Configuration** tab.
6. On the **Directory > Cognos** page, click the link for the **OpenPages DataSource**.
7. On the **Directory > Cognos > <data-source-name>** page, do the following:
 - a) Under the **Actions** column, click the **Set properties - OpenPages DataSource** icon .
 - b) On the **Set properties - OpenPages DataSource** page, click the **Connection** tab.
8. On the **Connection** tab, do the following:
 - a) Next to the **Connection String** box, click the pencil icon.
 - b) On the **OCI** tab, on the **Edit the connection string - Oracle** page, edit the SID value in the **SQL*Net connect string** field.
 - c) On the **JDBC** tab, edit the values in the **Server name**, **Port number**, and **Oracle Service ID** boxes.
9. For the Oracle Database environments, return to the **Directory > Cognos** page, and click the link for the **Oracle Native Driver** and repeat Steps 7-8 for the Oracle Native Driver.
10. Restart all administrative and managed servers.

Modifying database reference in the Cognos backup and restore environment file (Oracle only)

You must modify Oracle database references in the Cognos backup and restore environment file. This task applies only to Oracle database environments.

Procedure

1. Open a command or shell window and go to the `<CC_Home>|tools|bin` directory.
2. Locate the `op-cc-backup-restore.env` file in the `bin` directory and do the following tasks:
 - a) Make a backup copy of the file before you modify it.
 - b) Open the file in a text editor of your choice.

- c) Search the file for the string DB_ALIAS.
- d) Change the value that follows the equal sign to the new Cognos database alias. The format might look similar to the following example:

```
DB_ALIAS=<CommandCenter Database Alias>
```

Example

```
DB_ALIAS=OP
```

- e) Save your changes and exit the editor.
3. Restart the reporting server.
 4. Repeat these steps on each reporting server (active and standby).

Modifying database connection references in Cognos Configuration

You can modify database connection references in IBM Cognos Configuration.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
Note: For a Linux server, log on as a non-root user.
2. Start the IBM Cognos Configuration tool:
 - a) Open a Command Prompt window (using the **Run as administrator** option), or a Linux shell and navigate to the `<Cognos_Home>\bin64` directory.
 - b) Run one of the following commands to open the tool:
Windows:
`cogconfig.bat`
Linux:
`./cogconfig.sh`
3. In the **Explorer** pane, do the following steps:
 - a) Expand **Data Access** (if not already expanded).
 - b) Under **Content Manager**, click **Content store**.
4. In the properties pane, modify the values for the following properties:
 - a) Database server and port number (for example, eng11:1527).
 - b) User ID and password
 - c) Service name (for example, OP).
5. When finished, exit from Cognos Configuration.
6. Restart the Cognos server to effect the changes.
For more information, see [“Starting and stopping the Cognos services” on page 849](#).

TLS for OpenPages with Watson environments

You can configure OpenPages with Watson to use Transport Layer Security (TLS).

TLS establishes an encrypted link between the application server and web browsers, and between the application server and the other servers with which it communicates, such as the database server. The encryption ensures that all data that is passed between them remains private.

By default, OpenPages with Watson uses the TLSv1.2 protocol.

You can change the list of cipher suites that are enabled in IBM WebSphere Liberty. For more information, see the [Liberty documentation](#).

For information about the cipher suites that are supported by Java, see the [Java documentation](#).

Accessing the OpenPages with Watson application using TLS

You can access the IBM OpenPages with Watson application using a secure TLS connection. This procedure assumes that the default settings were not changed during installation.

Note: You must have an TLS digital certificate to use TLS with IBM OpenPages with Watson.

Open a browser window, and enter the following URL:

```
https://<server_name>:<tls_port>/openpages
```

Where <server_name> is the name of the server that hosts the OpenPages with Watson application, and <tls_port> is the TLS port number of the server.

For example:

```
https://server01.com:10111/openpages
```

Verifying TLS ports on application servers

Verify application ports in the <OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties on each horizontal cluster member.

Procedure

1. Log on to the application server.
2. Open the following file in a text editor: <OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties

Where <server_name> is the name of the application server.

3. Check that the HTTPS port is correct.

For example:

```
op.https.port=10111
```

4. If any HTTPS ports are missing, add them.
 5. Save your changes.
 6. Repeat these steps on each horizontal application server.
 7. Restart the application servers.
- For more information, see [“Starting application servers” on page 841](#).

Generating a Certificate Signing Request file

If you require an authorized certificate from a third-party certificate authority (CA), you can use Keytool to generate the required certificate signing request (CSR). Keytool is provided with IBM SDK, Java Technology Edition.

About this task

Use the `keytool -certreq` command to generate a CSR file. Contact your CA for information about their requirements for the CSR file. For information about `-certreq`, see `-certreq` in the IBM SDK, Java Technology Edition documentation.

The default location of the keystore on application servers is <OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security/key.p12

Importing signed CA certificates

You must install a root certificate and a server certificate from a trusted third-party certificate authority (CA) on each application server. You might also need to install an intermediate certificate on each

application server. You can use Keytool to import these certificates on the cluster administrator server and all cluster member systems. Keytool is provided with IBM SDK, Java Technology Edition.

Do this step after you receive the certificate from the Certificate Authority (CA). Use an ASCII PEM encoded certificate.

Use the `keytool -importcert` command to import the certificate. For more information, see [Importing a Certificate Reply](#) and `-importcert`.

The default location of the keystore on application servers is `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security/key.p12`

Procedure

1. Get the certificates from your CA and copy them to the OpenPages with Watson application server.
2. Log on to the OpenPages with Watson application server.
3. Import the certificate to WebSphere Liberty by running the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -trustcacerts -file <CERTIFICATE_NAME>
-keystore <STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- `<CERTIFICATE_ALIAS>` type an alias for the certificate.
- `<CERTIFICATE_NAME>` is the file name of the certificate.
- `<STORE_PATH>` is the full path and file name of the Liberty keystore on the application server. For example: `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security/key.p12`
- `<STORE_PASSWORD>` is the password of the Liberty keystore on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

4. Restart the OpenPages with Watson services.

What to do next

After you import the CA certificates, configure the application properties files to use the TLS protocol. Do the following tasks:

- [“Updating properties files so web browsers use the HTTPS protocol and TLS ports” on page 786](#)
- [“Configuring Cognos to connect to OpenPages by using TLS” on page 798](#)

After you install new server certificates, you might need to install the CA root and intermediate certificates into several additional locations, if the certificates are not from a trusted third party. For example, if the certificate authority is an internal authority for your enterprise, or you are using self-signed certificates, you need to do additional steps. Do the following tasks:

- [“Importing the CA certificate for the Java Runtime Environment of Cognos Analytics” on page 785](#)
- [“Installing CA certificates for all client browsers” on page 785](#)

Importing the CA certificate for the Java Runtime Environment of Cognos Analytics

Use the Keytool command to import the Certificate Authority (CA) certificate that issued the certificates for IBM OpenPages with Watson into the Java JRE environment on each reporting server.

Before you begin

On each reporting server, `$JAVA_HOME/bin` must be set in the PATH system environment variable. To verify that Java is in the PATH variable, run the following command:

```
java -version
```

If you get the following error, Java is not in the PATH variable: `Command not found`.

Procedure

1. Log on to each Cognos Analytics server as a user with administrative privileges.
2. Open a shell or command prompt. If you are using Windows, open the command prompt as an administrator.
3. Type the following Keytool command to import the OpenPages root certificate into the `cacerts` keystore.

```
keytool -importcert -alias <certificate_name> -trustcacerts  
-file <file_name> -keystore <keystore_name>
```

For example, the following Keytool command imports the `rootca` certificate from the `trustedcafilename.cer` file into the `cacerts` keystore file:

```
keytool -importcert -alias rootca -trustcacerts  
-file trustedcafilename.cer -keystore cacerts
```

4. Enter the password for the keystore.

The default password is `changeit`.

5. Enter Yes to trust the certificate.

What to do next

If you are using self-signed certificates for OpenPages that are not issued by a known CA, you must import the self-signed root certificate from any OpenPages server connected to the current Cognos server. Use the following Java keytool command to import the certificates into the keystore.

```
keytool -importcert -alias <certificate_name> -trustcacerts -file <file_name>  
-keystore <keystore_name>
```

Installing CA certificates for all client browsers

If your organization uses its own certificate authority (CA), most browsers will not trust the certificates. After you configure the web server for TLS, browsers might display a certificate exception. Users must accept the exception to access OpenPages.

Updating properties files so web browsers use the HTTPS protocol and TLS ports

After you configure the web server for TLS, edit the properties files to ensure that browsers use the HTTPS protocol and TLS ports. Do this task on the admin application server and all non-admin application servers.

About this task

In a load balanced environment, the values are the fully qualified domain name of the load balancer and its port number.

Procedure

1. Log on to each IBM OpenPages with Watson application server as a user with administrative privileges.
2. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
3. Go to the `<OP_HOME>/aurora/conf` directory.
4. Open the `aurora.properties` file in a text editor.

- a) Edit the following lines. Change `http` to `https` and change `<port>` to the TLS port number.

```
application.url.path=http://<server_name>:<port>/openpages
cognos.server=http://<server_name>:<port>/ibmcognos/cgi-bin/cognos.cgi
logout.url.cognos=http://<server_name>:<port>/ibmcognos/cgi-bin
cognos.cgi?b_action=xts.run&m=portal/logoff.xts&h_CAM_action=logoff
```

For example, in a load balanced environment, the `application.url.path` value is the fully qualified domain name of the load balancer and its port number.

- b) Save and close the file.
5. Open each `Server<#>-sosa.properties` file in a text editor.
 - a) Edit the following lines. Change `http` to `https` and change `<port>` to the TLS port number.

```
application.url.path=http://<server>:<port>/openpages
```

Note: In a load-balanced environment, this value is the fully qualified domain name of the load balancer and port.

- b) Save and close the file.
6. Open each `Server<#>-server.properties` in a text editor.
 - a) Edit the following lines. Change the `http` to `https` and change `<port>` to the TLS port number.

```
url.path.openpages=http://<server>:<port>/openpages
webclient.http.server.protocol=http
webclient.http.server.port=<port>
```

- b) Save and close the file.
7. Restart all OpenPages application servers.
- For more information, see [Chapter 24, "Starting and stopping servers,"](#) on page 841.

Enabling secure session cookies on WebSphere Liberty

Enable or disable the `cookieSecure` setting on all application servers in your environment.

A secure session cookie informs the browser to send the session cookie back only over an encrypted HTTP connection. This ensures that the cookie identifier is secure and is used only with IBM OpenPages with Watson when using HTTPS connections. When this feature is enabled, session cookies over an HTTP connection no longer work.

Procedure

1. Log on to the application server.
2. Edit the following file:
`<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/configDropins/overrides/op-apps.xml`
3. Locate the `httpSession` element. If it does not exist, create it.
4. Add the `cookieSecure` attribute to the `httpSession` element.
For example:

```
<httpSession cookieSecure="true" />
```

5. Locate the `webAppSecurity` element. If it does not exist, create it.
6. Add the `ssoRequiresSSL` attribute to the `webAppSecurity` element.
For example:

```
<webAppSecurity ssoRequiresSSL="true"/>
```

7. Restart the application server.
8. Repeat these steps on each application server.

TLS configuration for Microsoft Internet Information Services

In most environments, traffic to and from Cognos Analytics passes through a web server. You can configure the Microsoft Internet Information Services web server for TLS. Microsoft Internet Information Services requires a certificates snap-in.

Procedure

1. Log on to each Cognos Analytics server as a user with administrative privileges.
2. Start the Microsoft Management Console.
In the search box on the taskbar, type `mmc`, and press **Enter**.
3. In the **MMC** dialog box, click **File > Add/Remove Snap-Ins**.
4. In the **Available snap-ins** list, double-click **Certificates**.
5. In the **Certificates Snap-ins** dialog box, select **Computer account**, and then click **Next**.
6. In the **Select Computer** dialog box, select **Local Computer**, and then click **Finish**.
7. Click **OK** to close the dialog box.

Generating a key pair and request using Microsoft Internet Information Services

Use the reporting server to generate the key pair and specify the keystore in Microsoft Internet Information Services

Procedure

1. Log on to the primary reporting server as a user with administrative privileges.
2. In the Microsoft Management Console dialog box on the reporting server, expand the **Certificates** and select **Personal**.
3. In the **Actions** panel, right-click the **Certificates** icon and select **All Tasks > Advanced Options > Create Custom Request**.
4. In the **Certificate Enrollment** dialog box, click **Next**.
5. On the **Select Certificate Enrollment Policy** pane, select **Proceed without enrollment policy**, and click **Next**

6. On the **Custom request** pane, accept the default values of **CNG key** and **PKCS#10**, and click **Next**.
7. In the **Certificate Information** pane, click the **Details** icon, and click **Properties**.
8. In the **Certificate Properties** dialog box, click the **Subject** tab to supply details for the certificate's Distinguished Name.
9. To specify a common name and organization value.
 - a) In the **Type** list, select **Common Name**, and enter a value for the certificate common name, and click **Add**.
 - b) Select **Organization** in the **Type** list and enter a value for the certificate common name, and click **Add**.
10. Click the **Private Key** tab and then:
 - a) Click the arrow next to **Key Options**, and select **Make private key exportable**.
 - b) Click the arrow next to **Select Hash Algorithm**, select **sha1** from the **Hash Algorithm** list, and click **OK**.
11. In the **Certificate Information** pane, click **Next**.
12. In the **Certificate Enrollment** pane:
 - a) Click **Browse** and in the **Save as** dialog box, enter a name for the certificate request file in the **File name** field. Use a **.csr** extension.
 - b) From the **Save as type** list, select **All Files**, and then click **Save**.
13. Click **Finish**.
14. Close the Microsoft Management Console.

Submitting a Certificate Signing Request for your web server

Submit the Certificate Signing Request to a Certificate Authority for approval.

Procedure

1. Download the approved root and server certificates to a local directory, such as the OpenPagesDomain directory.
2. Check that the certificates are named to distinguish the root from the server certificate.
3. Follow the instructions provided by the Certificate Authority.

Importing the root certificate into Microsoft Internet Information Services

You must import the root certificate into Microsoft Internet Information Services on the primary Cognos system and all secondary Cognos systems.

Procedure

1. Log on to each Cognos server as a user with administrative privileges.
2. Start the Microsoft Management Console (MMC).
 - a) Click the Windows **Start** menu.
 - b) Type **mmc** in the search box and press **Enter**.
3. In the **MMC** dialog box, click **File > Add/Remove Snap-Ins**.
4. In the **Available snap-ins** list, double-click **Certificates**.
5. In the **Certificates Snap-ins** dialog box, select **Computer account**, and click **Next**.
6. In the **Select Computer** dialog box, select **Local Computer**, and click **Finish**.
7. In the **MMC** dialog box, expand **Certificates** and select **Trusted Root Certification Authorities**.
8. In the **Actions** panel, right-click the **Certificates** icon and select **All Tasks > Import**.
9. In the Certificate Import wizard, click **Next**.
10. On the **File to Import** pane, click **Browse** to locate the CA certificate, and then click **Next**.

11. On the **Certificate Store** pane, select **Place all certificates in the following store > Trusted Root Certification Authorities**, and click **Next**.
12. On the **Completing the Certificate Import** wizard screen, click **Finish**.
13. Repeat these steps to import any intermediate certificates required by your Certificate Authority.

What to do next

If you are using self-signed certificates for OpenPages with Watson and Cognos, that are not issued by a known Certificate Authority, you must import the OpenPages signed root certificate from any OpenPages server connected to the current Cognos server. Use the following Java keytool command to import the certificates into the keystore.

```
keytool -importcert -alias certificate_name -trustcacerts -file file_name
-keystore keystore_name
```

Adding the TLS binding for Microsoft Internet Information Services

To bind the root certificate to the web server use Cognos on the primary Cognos system and all secondary Cognos systems.

Procedure

1. On the Cognos server, open the Windows Internet Information Services Manager.
Click **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand the folder structure for the server that you want to configure, and then select **Sites**.
3. In the **Sites** pane, select the website to configure.
4. In the **Action** panel, select **Bindings**.
5. In the **Site Bindings** dialog box, select **HTTPS** and click **Edit**.

TLS configuration for Apache Web Server

To use TLS between IBM OpenPages with Watson applications and Apache Web Server, some configuration is required. For example, you must generate a keystore and a keypair, generate a certificate signing request, and establish the root of trust.

Generating a key pair and request using Cognos

Use Cognos to generate the key pair and specify the keystore for Apache Web Server on the primary Cognos system.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
Note: For Linux systems, log in as a non-root user, such as the `opuser` user that you created for the IBM OpenPages with Watson installation.
2. Open a Linux shell, or Windows command prompt.
3. Go to the `bin` directory in the web server home directory.
4. Enter the following commands to generate a certificate request:

Windows:

```
openssl req -new -sha1 -newkey rsa:1024 -config %APACHE_HOME%\conf\
openssl.cnf -nodes -keyout server_pkey.key
-out certreq.csr
```

Linux:

```
openssl req -new -sha1 -newkey rsa:1024 -config $APACHE_HOME/conf/
```

```
openssl.cnf -nodes -keyout server_pkey.key  
-out certreq.csr
```

5. Open the `httpd.conf` file using a text editor.
 - a) Uncomment the following line.

```
LoadModule ssl_module modules/mod_ssl.so  
Secure (SSL/TLS) connections  
Include conf/extra/httpd-ssl.conf
```

6. Save and close the file.

Submitting a Certificate Signing Request for your web server

Submit the Certificate Signing Request to a Certificate Authority for approval.

Procedure

1. Download the approved root and server certificates to a local directory, such as the `OpenPagesDomain` directory.
2. Check that the certificates are named to distinguish the root from the server certificate.
3. Follow the instructions provided by the Certificate Authority.

Importing the root certificate into Apache web server

You must import the root certificate into Apache web server on the primary Cognos system and all secondary Cognos systems.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
Note: Log on as a non-root user, such as the `opuser` user you created for the IBM OpenPages with Watson installation.
2. Go to the `<Apache_Home>/conf/extra` directory.
3. Open the `httpd-ssl.conf` file in a text editor.
4. Under **Server Certificate**, uncomment the **SSLCertificateFile** parameter, and enter the path to the PEM encoded certificate.
5. Under **Server Private Key**, uncomment the **SSLCertificateKeyFile** parameter, and enter the path to the keyfile on this server.
6. Under **Certificate Authority (CA)**, uncomment the **SSLCACertificateFile** parameter, and enter the path to the root certificate.
7. Save and close the file.

What to do next

If you are using self-signed certificates for OpenPages and Cognos that are not issued by a known Certificate Authority, you must import the OpenPages self-signed root certificate from any OpenPages server connected to the current Cognos server. Use the following Java **keytool** command to import the certificates into the keystore.

```
keytool -importcert -alias certificate_name -trustcacerts -file file_name  
-keystore keystore_name
```


Importing the server certificate into Apache web server

You must import the server certificate from the Certificate Authority into Apache web server on the primary Cognos system and all secondary Cognos systems.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
Note: Log on as a non-root user, such as the `opuser` user you created for the IBM OpenPages with Watson installation.
2. Go to the `<Apache_Home>/conf/extra` directory.
3. Open the `httpd-ssl.conf` file in a text editor.
4. Under **Server Certificate**, uncomment the **SSLCertificateFile** parameter, and enter the path to the PEM encoded certificate.
5. Under **Server Private Key**, uncomment the **SSLCertificateKeyFile** parameter, and enter the path to the keyfile on this server.
6. Under **Certificate Authority (CA)**, uncomment the **SSLCACertificateFile** parameter, and enter the path to the root certificate.

TLS configuration on a Linux load balancer server

To use TLS on a Linux-based load-balancing server that is running IBM HTTP Server (IHS) in IBM OpenPages with Watson, some configuration is required. For example, you must generate a keystore and a keypair, and generate a certificate signing request, and establish the root of trust.

Generating a keystore and key pair using the iKeyman tool

If you are using IBM HTTP Server as your web server, generate a key pair using the iKeyman tool on the load balance server.

Procedure

1. Log on to the load balance server as a user with administrative privileges.
2. Start iKeyman by running the following command:

```
IHS_root/bin/ikeyman
```

Where *IHS_root* is the location of the IHS.

The default location is *IHS_root* is `/usr/IBM/HTTPServer/`.
3. Create the keystore file to store the key pair.
 - a) Select **Key Database File > New**.
 - b) In the dialog box that displays, select **CMS** from the **Key database type** list.
 - c) In the **File Name** field, enter a file name for the new key database file.
 - d) In the **Location** field, enter the location where you want to store the keystore file, and click **OK**
For example: `usr/IBM/HTTPServer/bin`.
 - e) In the **Password Prompt** dialog box that displays, enter a password for the keystore. Re-enter the password.
 - f) In iKeyman, select **Stash password to file** to create a `.sth` file. This file encrypts and stores the keystore password which is assigned an expiration time. You must change the password periodically.
 - g) Click **OK**.

Generating a certificate signing request file using the iKeyman tool

If you require an authorized certificate from a trusted third-party certificate authority, you can use the iKeyman tool to generate the required certificate signing request.

Procedure

1. Log on to the load balance server as a user with administrative privileges.
2. Start iKeyman by running the following command: `IHS_root/bin/ikeyman`
Where *IHS_root* is the location of the IBM HTTP Server installation. The default location is `/usr/IBM/HTTPServer/`.
3. In the iKeyman tool, open the keystore created in Step 2.
 - a) Select **Key Database File > Open**.
 - b) Specify the type of keystore. The default type is **CMS**.
 - c) In the **File Name** and **Location** fields, enter the name and path to the keystore. You can also click **Browse** to locate the keystore, and click **OK**.
 - d) In the **Password Prompt** dialog box, enter the password for the keystore, and click **OK**.
4. Generate the certificate request for the open keystore.
 - a) Select **Create > New Certificate Request**.
 - b) In the **Create New Key and Certificate Request** dialog box, in the **Key Label** field, provide an identifier for the certificate.
 - c) In the **Key Size** list, select a key length for the certificate. The key size determines the strength of the encryption.
 - d) From the **Signature Algorithm** list, select an algorithm to apply to the certificate.
 - e) Provide the **dname** information to identify the certificate. Enter the values as appropriate.
 - commonName
 - organization
 - organizationUnit
 - localityName
 - stateName
 - country
 - f) Click **OK** to generate the request. A certificate request in the `.pem` format is created and saved to the specified location.

Submitting a Certificate Signing Request to a Certificate Authority running IBM HTTP

To submit the Certificate Signing Request, follow the instructions that are provided by the Certificate Authority. Depending on the instructions, you need to either copy and paste the content of the CSR to the text area or attach the CSR file.

Importing the Root and Signed Server Certificates using the iKeyman tool

You must install a signed certificate from a third-party certificate authority or self-signed certificates in both the keystore created and the keystore used by IBM HTTP Server. You must install a server certificate into the keystore created.

Procedure

1. Log on to the load balance server as a user with administrative privileges.
2. Start iKeyman by running the following command: `IHS_root/bin/ikeyman`
Where *IHS_root* is the location of the IHS. The default location is `/usr/IBM/HTTPServer/`.
3. In the iKeyman tool, open the keystore you created in Step 2.

- a) Select **Key Database File > Open**.
- b) Specify the type of keystore, by default **CMS**.
- c) In the **File Name** and **Location** fields, enter the name and path to the keystore.
- d) In the **Password Prompt** dialog box, enter the password for the keystore.
4. Import the signed CA certificate.
 - a) In the **Key database content** list, select **Signer Certificates**, and click **Add**.
 - b) In the **Open** window, in the **File Name** and **Location** fields, enter the name and path to the keystore.
 - c) In the **Enter a Label** dialog box that displays, in the **Enter a label for the certificate** field, enter a name for the certificate.
5. Select **Key Database File > Close**.
6. In the iKeyman tool, open the `plugin-key.kdb` keystore.
 - a) Select **Key Database File > Open**.
 - b) Specify the type of keystore. The default type is CMS.
 - c) In the **File Name** and **Location** fields, enter the name and path to the keystore.
 The default directory for the `plugin-key.kdb` keystore is `<IHS root>/Plugins/config/server_name/plugin-key.kdb`, and click **OK**.
 - d) In the Password Prompt dialog box, enter the password for the keystore. The default password is **WebAS**, and click **OK**.
7. Select **Signer Certificates** in the **Key database content** list, and click **Add**.
8. In the **Add CA's Certificate from a file** window, enter the following information.
9. In the **Data type** list, select Base64-encoded ASCII data.
10. In the **File Name** and **Location** fields, enter the name and path to the keystore.
11. In the **Enter a Label** dialog box and the **Enter a label for the certificate** field, enter a name for the certificate.

Editing the Apache configuration file on IBM HTTP server

You must edit the `httpd.conf` file on the load balancer server for the IBM HTTP server.

Procedure

1. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
2. Go to the `<IHS root>/conf` directory.
3. Open the `httpd.conf` file in a text editor.
 - a) Uncomment the following in the file.

```
LoadModule was_app22_module modules/mod_was_ap22_http.so
LoadModule negotiation_module module8s/mod_negotiation.so
```
 - b) Uncomment the following lines in the file and add any missing lines.

```
Listen 443
<VirtualHost *:443>
  ServerName <server_name>
  SSLEnable
  SSLProtocolDisable SSLv2
  SSLClientAuth None
  <Directory />
    Options FollowSymLinks
    AllowOverride None
    Order allow,deny
```

```

Allow from all
</Directory>
</VirtualHost>
SSLDisable
KeyFile <IHS_root>/<keystore_name>.kdb

```

- c) Add the following line to point to the WebSphere plug-in Configuration.

```

WebSpherePluginConfig
<IHS root>/Plugins/config/<server_name>/plugin-cfg.xml

```

- d) Save and close the file.

4. To apply the changes, restart the IBM HTTP Server.

TLS configuration for CommandCenter for an Apache load balancer server (Windows)

There are four procedures for the web server on any reporting server that handles external IBM OpenPages with Watson CommandCenter requests.

Generating a key pair and request with an Apache load balancer server

If you are using Apache as your load balancer server, you must generate a key pair and specify the keystore.

Procedure

1. Log on to the load-balancing server as a non-root user with administrative privileges.
2. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
3. Go to the \bin directory in the web server home directory to use as the keystore.
4. To generate a certificate request, enter the following command :

- For Windows operating systems:

```

openssl req -new -sha1 -newkey rsa:1024 -config %APACHE_HOME%
\conf\openssl.cnf
-nodes -keyout server_pkey.key -out certreq.csr

```

- For Linux operating systems:

```

openssl req -new -sha1 -newkey rsa:1024 -config
$APACHE_HOME\conf\openssl.cnf
-nodes -keyout server_pkey.key -out certreq.csr

```

5. Open the httpd.conf file in a text editor and uncomment following line:

```

LoadModule ssl_module modules/mod_ssl.so
Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf

```

Submitting a CSR to a Certificate Authority for an Apache load balancer server

Submit the Certificate Signing Request (CSR) file for an Apache load balancer server to an appropriate Certification Authority (CA) for approval.

Procedure

1. Download the approved root and server certificates to a local directory, such as the OpenPagesDomain directory.
2. Check that the certificates are named to distinguish the root from the server certificate.

3. Follow the instructions provided by the Certificate Authority.

Importing the root certificates for an Apache load balancer server

You must import the root certificates into an Apache load balancer server.

Procedure

1. Log on to the load-balancing server as a non-root user with administrative privileges.
2. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
3. Go to the `<Apache_Home>/conf/extra` directory.
4. Open the `httpd-ssl.conf` file in a text editor.
5. Under **Server Certificate**, uncomment the **SSLCertificateFile** parameter, and enter the path to the PEM encoded certificate.
6. Under **Server Private Key**, uncomment the **SSLCertificateKeyFile** parameter, and enter the path to the key file on this server.
7. Under **Certificate Authority (CA)**, uncomment the **SSLCACertificateFile** parameter, and enter the path to the root certificate.
8. Save and close the file.

Editing the Apache configuration file on Apache load balancer server

To add TLS parameters for the Apache load balancer server, you must edit the `httpd.conf` file.

Procedure

1. Log on to load-balancing web server as a user with administrative privileges.
2. Stop the Apache web server.
3. Start a Command Prompt window by using the **Run as administrator** option.
4. Copy the `<WL_Home>\server\plugin\win\32\mod_wl_22.so` file to the `Apache_Home\modules` directory.
Copy `C:\Oracle\Middleware\wlserver_10.3\server\plugin\win\32\mod_wl_22.so` to `C:\Program Files\Apache Software Foundation\Apache2.2\conf`
5. Go to the `<Apache_Home>\conf\` directory.
6. Open the `httpd.conf` file and locate the parameters added to the end of the file for SSL. See the following example of these parameters.
 - a) Before the first **<Location />** parameter, add the following parameter.

```
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
```
 - b) In the **<Location />** parameter, add the location of the trusted CA certificate file.

TLS configuration for Cognos for IBM HTTP Server

If you use IBM HTTP Server (IHS) as a web server for Cognos, some configuration is required. For example, you must generate a keystore and key pair, and generate a certificate signing request, and submit a Certificate Signing Request (CSR).

Generating a keystore and key pair using the iKeyman tool

If you are using IBM HTTP Server as your web server, generate a key pair using the iKeyman tool on the reporting server.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start iKeyman by running the following command:

```
IHS_root/bin/ikeyman
```

Where *IHS_root* is the location of the IHS.

The default location is *IHS_root* is `/usr/IBM/HTTPServer/`.

3. Create the keystore file to store the key pair.

- a) Select **Key Database File > New**.

- b) In the dialog box that displays, select **CMS** from the **Key database type** list.

- c) In the **File Name** field, enter a file name for the new key database file.

- d) In the **Location** field, enter the location where you want to store the keystore file, and click **OK**

For example: `usr/IBM/HTTPServer/bin`.

- e) In the **Password Prompt** dialog box that displays, enter a password for the keystore. Re-enter the password.

- f) In iKeyman, select **Stash password to file** to create a `.sth` file. This file encrypts and stores the keystore password which is assigned an expiration time. You must change the password periodically.

- g) Click **OK**.

Generating a certificate signing request file using the iKeyman tool

If you require an authorized certificate from a trusted third-party certificate authority, you can use the iKeyman tool to generate the required Certificate Signing Request.

Procedure

1. Log on to the reporting server as a user with administrative privileges.

2. Start iKeyman by running the following command: *IHS_root*/bin/ikeyman

Where *IHS_root* is the location of the IBM HTTP Server installation. The default location is `/usr/IBM/HTTPServer/`.

3. In the iKeyman tool, open the keystore created in Step 2.

- a) Select **Key Database File > Open**.

- b) Specify the type of keystore. The default type is **CMS**.

- c) In the **File Name** and **Location** fields, enter the name and path to the keystore. You can also click **Browse** to locate the keystore, and click **OK**.

- d) In the **Password Prompt** dialog box, enter the password for the keystore, and click **OK**.

4. Generate the certificate request for the open keystore.

- a) Select **Create > New Certificate Request**.

- b) In the **Create New Key and Certificate Request** dialog box, in the **Key Label** field, provide an identifier for the certificate.
- c) In the **Key Size** list, select a key length for the certificate. The key size determines the strength of the encryption.
- d) From the **Signature Algorithm** list, select an algorithm to apply to the certificate.
- e) Provide the **dname** information to identify the certificate. Enter the values as appropriate.
 - commonName
 - organization
 - organizationUnit
 - localityName
 - stateName
 - country
- f) Click **OK** to generate the request. A certificate request in the .arm format is created and saved to the specified location.

Submitting a CSR to a Certificate Authority

To submit the Certificate Signing Request, follow the instructions that are provided by the Certificate Authority. Depending on the instructions, you need to either copy and paste the content of the CSR to the text area or attach the CSR file.

Downloading and importing the root and signed server certificates using the iKeyman tool

You must install a signed certificate from a third-party Certificate Authority or self-signed certificates in both the keystore created and the keystore used by IBM HTTP Server. You must install a server certificate into the keystore created.

Procedure

1. Follow the instructions provided by the Certificate Authority to download the root and signed server certificates.
2. Download the approved root and Certificate Authority certificates to a local directory.
3. Check that the certificates are named to distinguish the root from the Certificate Authority certificate.
4. Log on to the reporting server as a user with administrative privileges.
5. Start iKeyman by running the following command: `<IHS_root>/bin/ikeyman`
Where `<IHS_root>` is the location of the IHS. The default location is `/usr/IBM/HTTPServer/`.
6. In the iKeyman tool, open the keystore you created for Cognos.
 - a) Select **Key Database File > Open**.
 - b) Specify the type of keystore, by default **CMS**.
 - c) In the **File Name** and **Location** fields, enter the name and path to the keystore.
 - d) In the **Password Prompt** dialog box, enter the password for the keystore.
7. Import the root certificate.
 - a) In the **Key database content** list, select **Signer Certificates**, and click **Add**.
 - b) In the **Open** window, in the **File Name** and **Location** fields, enter the name and path to the root certificate file.
 - c) In the **Enter a Label** dialog box that displays, in the **Enter a label for the certificate** field, enter a name for the root certificate.
8. Import CA signed certificate.
 - a) In the **Key database content** list, select **Personal Certificates**, and click **Receive**.

- b) In the **Open** window, in the **File Name** and **Location** fields, enter the name and path to the CA signed certificate file.
When the import is complete, a status message is displayed.
- c) Click **OK**.

Updating the Apache configuration file on IBM HTTP server

You must update the `httpd.conf` file and restart the server.

Procedure

1. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
2. Go to the `<IHS root>/conf` directory.
3. Open the `httpd.conf` file using a text editor.

- a) Uncomment the following in the file.

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 443
<VirtualHost *:443>
    SSLEnable
</VirtualHost>
KeyFile /home/opuser/IBM/HTTPServer/<yourkeystore.kdb>
SSLDisable
```

- b) Save and close the file.

Note: You must also replace `<yourkeystore.kdb>` with your keystore file and replace port 443 with your TLS/SSL port for IBM HTTP Server.

4. To apply the changes, restart the IBM HTTP Server.

Configuring Cognos to connect to OpenPages by using TLS

If IBM OpenPages with Watson is configured for TLS, you must configure the properties file to use the OpenPages HTTPS address and TLS port. Modify the OpenPages properties file to use HTTPS and the TLS port on the primary Cognos server and on each secondary Cognos server.

Before you begin

Set up IBM HTTP Server (IHS) as a web server for Cognos. For more information, see [“TLS configuration for Cognos for IBM HTTP Server”](#) on page 796.

Procedure

1. Log on to the Cognos server as a user with administrative privileges.
Note: For Linux, log on as a non-root user, such as the `opuser` user that you created for the OpenPages with Watson installation.
2. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
3. Go to the following directory: `<Cognos_Home>/configuration`
4. Open the `OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties` file in a text editor.
5. Edit the following lines to change the `http` to `https` and update the port number.

```
openpages.application.url=http\://<server>:<port>/openpages
```

6. Restart all Cognos servers.

For more information, see [Chapter 24, “Starting and stopping servers,” on page 841](#).

TLS configuration for Db2

You can configure a secure connection between IBM Db2 and IBM OpenPages with Watson.

You can configure a Transport Layer Security (TLS) connection between the database server and the application servers, and between the database server and the reporting servers.

You can also configure a secure connection between the database server and the search server. For more information, see [“Enabling a TLS database connection between the search server and the database server” on page 809](#).

Setting up SSL on the database server (Db2)

You can configure a secure connection between the OpenPages database on IBM Db2 and the OpenPages application servers. You can also set up a secure connection between the OpenPages database and Cognos. First, you need to set up SSL on Db2.

Procedure

1. Stop all application servers and all reporting servers.
2. Stop the OpenPages database.
 - a) Log on to the database server as the OpenPages database instance owner (by default db2inst1 on Linux or db2admin on Windows).
 - b) Run the following commands:

```
db2 deactivate db <op_database_name>
db2stop
```

Replace `<op_database_name>` with the name of the OpenPages database, for example opx.

3. Enable SSL (TLS) on the database server.

Do these steps as the OpenPages database instance owner.

- a) Create a directory for the database key.
- b) Go to `<DB2_HOME>/sqlllib/gskit/bin`.
- c) Run the following command:

```
gsk8capicmd_64 -keydb -create -db <keystore_directory>/<db_key_name>.p12 -pw
"<db_key_password>" -type pkcs12 -stash
```

- Replace `<keystore_directory>` with the directory that you created in step [“3.a” on page 799](#).
 - Replace `<db_key_name>` with the name of the keystore file (.p12).
 - Replace `<db_key_password>` with the password of the keystore.
- d) Go to the directory that you created in step [“3.a” on page 799](#) (the `<keystore_directory>`).
 - e) Add `<DB2_HOME>/sqlllib/gskit/bin` to the system path.
 - f) Do one of the following steps:
 - Run the following command:

```
gsk8capicmd_64 -cert -extract -db "<db_key_name>.p12" -pw "<db_key_password>" -label
"<certificate_name>" -target "<certificate_name>.arm" -format ascii -fips
```

Copy the certificate to the following directory on the application server: `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security/`

- Or, run the following command from the application server:

```
gsk8capicmd_64 -cert -create -db "<db_key_name>.p12" -pw "<db_key_password>"  
-label "<certificate_name>" -dn "CN=<host_name>, O=<company>, L=<city>, ST=<state>,  
C=<country>"
```

You now have a self-signed certificate for the OpenPages database.

4. Update Db2 configuration parameters.

- a) Run the following commands in the following sequence. Wait for each command to complete before you run the next command:

```
db2 update dbm cfg using SSL_SVR_KEYDB <keystore_directory>/<db_key_name>.p12  
db2 update dbm cfg using SSL_SVR_STASH <keystore_directory>/<db_key_name>.sth  
db2 update dbm cfg using SSL_SVR_LABEL <certificate_name>  
db2 update dbm cfg using ssl_svcsname <db2_ssl_port>  
db2set -i <db_user_name> DB2COMM=SSL,TCPIP
```

- b) If you have a second database server, repeat these steps on the second database server.

5. Start the OpenPages database.

- a) Log on to the database server as the OpenPages database instance owner (by default db2inst1 on Linux or db2admin on Windows).
- b) Run the following commands:

```
db2start  
db2 activate db <op_database_name>
```

6. Configure your firewall to allow connections to the SSL port for Db2.

What to do next

Configure WebSphere Liberty to connect to Db2 by using the secure connection. For more information, see [“Configuring application and reporting servers to use a secure connection to the database \(Db2\)” on page 800.](#)

Configuring application and reporting servers to use a secure connection to the database (Db2)

After you set up SSL on IBM Db2, configure WebSphere Liberty and Cognos to use the secure connection.

Before you begin

Ensure that you completed all steps in [“Setting up SSL on the database server \(Db2\)” on page 799.](#)

Ensure that you know the SSL port number for Db2.

Procedure

1. Log on to the admin application server as the OpenPages installation user (opuser).
2. If you do not have the SSL certificate for Db2, run the following command:

```
openssl s_client -servername <db_server_url> -connect <db_server_url>:<db_server_ssl_port>  
</dev/null 2>/dev/null | \  
sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > <directory>/db2.cert;
```

- Replace <db_server_url> with the fully qualified domain name (FQDN) of the database server.
 - Replace <db_server_ssl_port> with the SSL port for Db2.
 - Replace <directory> with the full path to a directory on the application server. This directory is where the certificate is saved.
3. Import the Db2 certificate to the Java keystore on the application server.
- For example:

```
/opt/ibm/java-x86_64-80/jre/bin/keytool -import \
  -alias db2_ssl \
  -trustcacerts \
  -file /home/opuser/db2.cert \
  -keystore /opt/ibm/java-x86_64-80/jre/lib/security/cacerts \
  -storepass <Java_password>
```

4. Import the Db2 certificate to the Liberty keystore on the application server.

If you are using vertical application servers, do this step on each of them.

For example:

```
/opt/ibm/java-x86_64-80/jre/bin/keytool -import \
  -alias db2_ssl \
  -trustcacerts \
  -file /home/opuser/db2.cert \
  -keystore /home/opuser/IBM/OpenPages/wlp-usr/servers/OpenPagesNodeServer1Server1/
resources/security/key.p12 \
  -storetype PKCS12 \
  -storepass <password>
```

5. Modify the op-db2.xml file.

- a) Copy the <OP_HOME>/wlp-usr/servers/<server_name>Server<#>/op-db2.xml file to the following directory: <OP_HOME>/wlp-usr/servers/<server_name>Server<#>/configDropins/overrides/.

Do not modify or delete the <OP_HOME>/wlp-usr/servers/<server_name>Server<#>/op-db2.xml file.

- b) Open the following file in a text editor: <OP_HOME>/wlp-usr/servers/<server_name>Server<#>/configDropins/overrides/op-db2.xml
- c) For each properties.db2.jcc property, append sslConnection="true"

For example:

```
<properties.db2.jcc autoCommit="false" databaseName="{op.db2.databaseName}"
enableExtendedDescribe="2" password="{op.jdbc.password}" portNumber="{
{op.db2.portNumber}" serverName="{op.jdbc.host}" user="{op.jdbc.user}"
sslConnection="true" />
```

6. Modify the bootstrap.properties file.

- a) Open the following file in a text editor: <OP_HOME>/wlp-usr/servers/<server_name>Server<#>/bootstrap.properties
- b) Update the op.db2.portNumber property with the SSL port number for Db2.

7. Modify the aurora.properties file.

- a) Open the following file in a text editor: <OP_HOME>/aurora/conf/aurora.properties
- b) Update the database.PORT property with the SSL port number for Db2.
- c) Update the database.URL property with the SSL port number for Db2.

Append :sslConnection=true; to the URL.

For example:

```
database.URL=jdbc\:db2\://op-appserver.ibm.com\:50001/OPX:sslConnection=true;
```

8. Configure the IBM Db2 database client to use the secure connection. Do this step on each application server and reporting server.

- a) Import the Db2 certificate to the Java keystore that is bundled with the Db2 client software.

For example:

```
/home/opuser/sqllib/java/jdk64/jre/bin/keytool -import \
  -alias db2_ssl \
  -trustcacerts \
  -file /home/opuser/db2.cert \
  -keystore /home/opuser/sqllib/java/jdk64/jre/lib/security/cacerts \
  -storepass <password>
```

- b) Create a keystore for the Db2 client.

For example:

```
gsk8capicmd -keydb -create -db /home/opuser/sqllib/security/keystore/opx_db.p12 -pw  
"OpenPages1" -type pkcs12 -stash  
db2 update dbm cfg using SSL_CLNT_KEYDB /home/opuser/sqllib/security/keystore/opx_db.p12  
db2 update dbm cfg using SSL_CLNT_STASH /home/opuser/sqllib/security/keystore/opx_db.sth
```

c) Import the Db2 certificate.

For example:

```
gsk8capicmd -cert \  
-add \  
-db /home/opuser/sqllib/security/keystore/opx_db.p12 \  
-stashed \  
-label db2_ssl \  
-file /home/opuser/db2.cert \  
-format ascii \  
-fips
```

9. Recatalog the OpenPages node.

For example:

```
db2 uncatalog node openpage  
db2 catalog TCP/IP NODE openpage REMOTE op-dbserver.com server 50001 SECURITY SSL  
db2cli writecfg add -dsn OPXSSL -database OPX -host op-dbserver.com -port 50001 -parameter  
'SecurityTransportMode=SSL'
```

10. Restart the OpenPages application services.

11. Repeat steps “1” on page 800 to “10” on page 802 on each application server.

12. Update the database connection information in Cognos so that the reporting servers use SSL to connect to the OpenPages database.

a) Open **IBM Cognos Administration**. Select the **OpenPages data source** and edit the connection string.

For more information, see [“Update Db2 database connection references for Cognos ” on page 700.](#)

b) Click the **JDBC** tab.

c) Change **Port number** to the SSL port number for Db2.

d) In the **JDBC Connection Parameter field**, type `sslConnection="true";`.

e) Save your changes and exit **IBM Cognos Administration**.

f) Restart the reporting servers.

Modifying the LDAP configuration file for LDAP over TLS

You must modify the authentication configuration file to enable the LDAP directory server that you are using.

The `aurora_auth.config` file contains three authentication modules:

- Openpages - the default internal user directory
- OpenpagesIP - a sample LDAP configuration for the Sun One Directory Server
- OpenpagesAD - a sample LDAP configuration for the Microsoft Active Directory Server

The only module that the IBM OpenPages with Watson system pays attention to is the module that is named Openpages. Therefore, you need to make a backup of the Openpages module, rename the OpenpagesIP or OpenpagesAD to Openpages, and then change the settings to reflect the settings of your LDAP server.

Procedure

1. Stop all OpenPages with Watson services.
2. Open and edit the `<OP_HOME>/aurora/conf/aurora_auth.config` file in a text editor.

Where:

<OP_HOME> is the installation location of the OpenPages with Watson application.

3. Find the Openpages module and change its name to OpenpagesDefault.
4. Modify either the OpenpagesIP or OpenpagesAD module name to Openpages.
 - If you are using a Microsoft Active Directory server, change the name of the OpenpagesAD module to Openpages.
 - If you are using a Sun One Directory Server, change the name of the OpenpagesIP module to Openpages.
 - If you are using a different LDAP server, you can use either of these modules. Choose a module to use as a template and change its name to Openpages.
5. Specify the correct values for the following properties in the module that you named Openpages:

provider.url

Change the value to the hostname and port number for the LDAP authentication server. For LDAP over TLS (LDAPS), the protocol is ldaps and the port is the LDAPS port number (by default, 636).

base.dn

The top level of the LDAP directory tree structure (Domain Name) on the LDAP server. If the users to be authenticated are located in multiple locations within your Active Directory structure, list all of the locations explicitly by using the distinguished names of the locations, each separated by a semi-colon.

For example:

```
base.dn="DC=LDAPTesting,DC=local;CN=Users,DC=LDAPTesting,DC=local;  
OU=Auditors,OU=External Auditors,OU=Staff,DC=LDAPTesting,DC=local"
```

user.attr.id

The attribute name of the user identifier (for example, uid, cn, etc.).

Additional custom parameters

You can add additional custom parameters that are supported by the Java Naming and Directory Interface (JNDI). Precede a JNDI property with the `ctx.env.` prefix.

For example, if you want to use the JNDI property `com.sun.jndi.ldap.connect.timeout`, use `ctx.env.com.sun.jndi.ldap.connect.timeout=<value>` in the `aurora_auth.config` file.

For information about JNDI properties, see the [Java SE documentation](#).

For example:

```
Openpages  
{  
  com.openpages.aurora.service.security.namespace.LDAPLoginModule  
    required debug=false  
    provider.url="ldaps://myserver.company.com:636"  
    security.authentication="simple"  
    security.search.user.dn="cn=Directory Manager"  
    security.search.user.credentials="openpages"  
    base.dn="ou=people,o=IBM,c=US"  
    user.attr.id="uid"  
  ;  
};
```

6. When you are finished editing the file, save your changes and exit.
7. Import the root certificate and any intermediate signer certificates for your LDAP server to the trust store on the OpenPages application servers.

For more information, see [“Importing signed CA certificates”](#) on page 783.
8. Restart all services.

Results

You have configured the OpenPages with Watson system to use an external LDAP user authentication server over TLS.

Renewing TLS certificates for OpenPages with Watson

Periodically, TLS certificates need to be renewed and re-imported into your IBM OpenPages with Watson environment.

The process for renewing a certificate is similar to the process for installing new certificates. You create a new certificate request and import the signed certificate into the appropriate keystores. You do not need to repeat the steps for configuring TLS and changing property files for OpenPages with Watson, unless information contained in the certificate changes.

Certification Authorities provide instructions on how to submit renewal applications and import the signed certificates.

Renewing TLS certificates for Cognos environments on an IIS Web Server

Renew TLS certificates for Cognos environments for the web server on any reporting server that handles external Cognos traffic.

This information applies only to Windows environments.

Procedure

1. Generate a key pair and request.
 - a) Log on to the reporting server as a user with administrative privileges.
 - b) Launch the Internet Information Services Manager, by clicking **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.
 - c) In the **Internet Information Services Manager**, select the application server you want to configure.
 - d) In the **Features** view, double-click **Server Certificates**.
 - e) In the **Actions** pane, click **Create Certificate Request** to launch the Request Certificate Wizard.
 - f) On the **Distinguished Name Properties** screen of the wizard:

Table 251. Distinguished Name Properties screen	
In this text box	Do this
Common name	Type a name for the certificate.
Organization	Type the name of the organization in which the certificate will be used.
Organizational unit	Type the name of the organizational unit in the organization in which the certificate will be used.
City/locality	Type the unabbreviated name of the city or locality where your organization or organizational unit is located.
State/province	Type the unabbreviated name of the state or province where your organization or organizational unit is located.

Table 251. Distinguished Name Properties screen (continued)	
In this text box	Do this
Country/region	Type the name of the country or region where your organization or organizational unit is located.

- g) Click **Next**.
 - h) On the **Cryptographic Service Provider Properties** screen, select a cryptographic service provider from the list:
 - Microsoft RSA SChannel Cryptographic Provider
 - Microsoft DH SChannel Cryptographic Provider
 - i) On the **Cryptographic Service Provider Properties** screen, select a bit length that can be used by the provider from the **Bit length** drop-down list.
 By default, the RSA SChannel provider uses a bit length of 1024. The DH SChannel provider uses a bit length of 512. A longer bit length is more secure, but it can affect performance.
 - j) Click **Next**.
 - k) On the **File Name** page, in the **Specify a file name for the certificate** request field, use the **Browse** icon or type a name for the certificate file.
 - l) Click **Finish**.
2. Submit the Certificate Signing Request (CSR) to the Certification Authority (CA) for approval.
 - a) Submit the CSR to your CA to renew the certificate. Follow the instructions provided by your CA on how to submit the CSR.
 - b) Download the approved root and CA certificates to a local directory. Make sure the certificates are named to distinguish the root from the CA certificate.
 3. Install the signed certificate.
 Import the renewed server certificate into each reporting server by performing the following tasks:
 - a) Log on to the reporting server as a user with administrative privileges.
 - b) Launch the Internet Information Services Manager, by clicking **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.
 - c) In the **Internet Information Services Manager**, select the application server you want to configure.
 - d) In the **Features** view, double-click **Server Certificates**.
 - e) In the **Actions** pane, click **Complete Certificate Request**.
 - f) On the **Complete Certificate Request** screen:
 - In the **File name that contains the certification authority's** response field, use the **Browse** icon or type the path of the file that contains the signed certificate.
 - In the **Friendly name** field, type a recognizable name for the certificate.
 - Click **OK**.

Renewing TLS certificates for Cognos environments on an Apache Web Server

Perform these steps for the web server on any reporting server that handles external Cognos traffic.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
Note: Log in as a non-root user, such as the user you created for the IBM OpenPages with Watson installation, for example: opuser.

2. Perform the following tasks to renew your certificate(s):
 - a) Generate a key pair and request.
 - b) Submit the CSR to the CA for approval.
 - c) Apache uses OpenSSL which requires the server keys and certificate locations be updated in `extras/httpd-ssl.conf`.

For more information, see [“TLS configuration for Apache Web Server” on page 789](#).

Renewing TLS certificates on application servers

To renew a TLS certificate for IBM OpenPages with Watson, create a new certificate signing request, submit it to a Certification Authority, and import the signed server certificate.

Procedure

1. Log on to cluster administrator server as a user with administrative privileges.
2. Create the certificate request.

For more information, see [“Generating a Certificate Signing Request file” on page 783](#).
3. Submit the request to the Certification Authority (CA).
 - a) Submit the Certificate Signing Request (CSR) to your Certification Authority (CA) to renew the certificate. Follow the instructions provided by your CA on how to submit the CSR.
 - b) Download the approved server and CA certificates. Make sure the certificates are named to distinguish the server from the CA certificate.
4. Import the certificate.

Import the renewed server certificate into each application server. For more information, see [“Importing signed CA certificates” on page 783](#).

Setting up a secure connection for the global search service

You can configure the IBM OpenPages with Watson global search service (Apache Solr) to use a secure connection with TLS. TLS ensures that all data that is passed between the application server and the Solr service remains private.

Before you begin

On the search server and application servers, `$JAVA_HOME/bin` must be set in the `PATH` system environment variable. To verify that Java is in the `PATH` variable, run the following command:

```
java -version
```

If you get the following error, Java is not in the `PATH` variable: `Command not found`.

About this task

If you are setting up the global search component in a test environment, do not enable TLS until you resolve all installation and configuration issues.

For more information about the commands that are used in this task, see the [Apache Solr Reference Guide](#).

Important: IBM is not responsible for third-party content. At the time of publication, the information is correct.

Procedure

1. If the global search component is enabled, you must disable it.
 - a) Log on to OpenPages as a user with administrative privileges. Go to the Standard UI.

- b) Click **Administration > Global Search**.
- c) Click **Disable**.

2. Stop the global search services.

For more information, see [“Start or stop the global search services” on page 844](#).

3. Create a certificate for the secure connection.

- a) Go to the `<SEARCH_HOME>/solr/server/etc` folder and run the following command.

```
keytool -genkeypair -alias alias -keyalg key_algorithm
-keysize keysize -keypass key_pass -storepass keystore_passwd
-validity validity -keystore jks_keystore -ext ip_address
-dname "CN=localhost, OU=Organizational Unit, O=Organization, L=Location,
ST=State, C=Country"
```

In the following example, the command creates a self-signed certificate in a key store named `solr-ssl.keystore.jks`. The key store contains a key with an alias of `solr-ssl`, a key store password of `secret`, a trust store password of `secret`. It specifies Subject Alternative Name (SAN) values of `DNS:host1.companya.com` and `IP:127.0.0.1,192.168.7.1` to include in the certificate. (SAN values are not mandatory, and might not be specified in your environment).

```
keytool -genkeypair -alias solr-ssl -keyalg RSA
-keysize 2048 -keypass secret -storepass secret
-validity 9999 -keystore solr-ssl.keystore.jks
-ext SAN=DNS:host1.companya.com,IP:127.0.0.1,IP:192.168.7.1
-dname "CN=localhost, OU=Organizational Unit, O=Organization, L=Location,
ST=State, C=Country"
```

- b) Convert the JKS key store into PKCS12 format.

```
keytool -importkeystore -srckeystore jks_keystore
-destkeystore jks_keystore.p12 -srcstoretype source_keystore_type
-deststoretype destination_keystore_type
```

When prompted, type a destination key store password, and the source key store password that you specified in the step 3a.

- c) Convert the PKCS12 format key store, including the certificate and the key, into PEM format.

To run this command, `openssl` must be installed, and added to the `PATH` environment variable.

```
openssl pkcs12 -in <jks_keystore.p12> -out <jks_keystore.pem>
```

When you are prompted for the import password and PEM pass phrase, you can use the same password that you specified for the `<key_pass>` value in step 3a.

4. Export the certificate.

```
keytool -exportcert -keystore <jks_keystore> -alias <alias> -file <solr_certificate>
```

When you are prompted for the key store password, type the password that you specified for the `<key_pass>` value in step 3a.

5. Update the `solr.in` file.

- a) Edit the following file in a text editor:

Windows

```
<SEARCH_HOME>\solr\bin\solr.in.cmd
```

Linux

```
<SEARCH_HOME>/solr/bin/solr.in.sh
```

- b) Uncomment and set the following TLS properties.

```
SOLR_SSL_KEY_STORE=etc/jks_keystore
SOLR_SSL_KEY_STORE_PASSWORD=keystore_passwd
SOLR_SSL_TRUST_STORE=etc/jks_keystore
SOLR_SSL_TRUST_STORE_PASSWORD=keystore_passwd
```

```
SOLR_SSL_NEED_CLIENT_AUTH=false
SOLR_SSL_WANT_CLIENT_AUTH=true
```

On Windows, you might need to use server/etc as the path name for the SOLR_SSL_KEY_STORE and SOLR_SSL_TRUST_STORE properties.

6. Log in to the OpenPages application as a user with administrative privileges.

7. Open the **Settings** page.

- In the Task Focused UI, click  > **System Configuration** > **Settings**.
- In the Standard UI, click **Administration** > **Settings**.

8. Update the following settings to use https instead of http.

Platform > Search > Admin > Search Server Administration URL

Platform > Search > Index > Search Server URL

Platform > Search > Request > Search Server URL

9. Copy the certificate file that you exported to the following directory on the application server.

<JAVA_HOME>/lib/security

10. Add the certificate to the IBM JRE key store file.

- a) On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
- b) Back up the <JAVA_HOME>/lib/security/cacerts file.
- c) Go to the <JAVA_HOME>/bin directory and run the following command.

```
keytool -importcert -alias <alias> -keystore cacerts -file <solr_certificate>
```

When prompted, type the key store password of the cacerts key store. The default password is typically changeit.

- d) Confirm that you want to trust the certificate.
- e) Restart all OpenPages services.

11. Import the certificate to the IBM WebSphere trust store.

- a) Log on to the OpenPages application server.
- b) Run the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_NAME> -keystore
<STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- <CERTIFICATE_ALIAS> is the alias of the certificate.
- <CERTIFICATE_NAME> is the file name of the certificate.
- <STORE_PATH> is the full path and file name of the trust store on the application server.
For example: /opt/IBM/OpenPages/wlp-user/servers/<server_name>Server<#>/resources/security/key.p12
- <STORE_PASSWORD> is the password of the trust store on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

- c) Restart all OpenPages services.

12. Start the global search services.

For more information, see [“Start or stop the global search services”](#) on page 844.

13. If the search server is installed on a different computer than the application server, add the certificate to the IBM JRE key store on the search server.

- a) On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
- b) Go to the <JAVA_HOME>/bin directory and run the following command:

```
keytool -importcert -alias <alias> -keystore cacerts -file <SEARCH_HOME>/solr/server/etc/solr_certificate
```

- c) When prompted, type the key store password of the cacerts keystore. The default password is typically changeit.

Enabling a TLS database connection between the search server and the database server

When you install the global search server, it uses a plain connection to communicate with the database server. If your organization requires that you use a TLS connection, you must complete these steps.

Procedure

1. Disable global search.
 - a) Log in to IBM OpenPages with Watson with administrative privileges. Go to the Standard UI.
 - b) Navigate to **Administration > Global Search** and select **Disable**.
2. Configure TLS on the database server.
3. On the search server, follow these steps to enable TLS:
 - a) If you are using Windows, open a command prompt with the **Run As administrator** option.
 - b) Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ directory.
 - c) Enable TLS by running the following command.

```
opsearchtool.cmd|.sh enableSSLDbConn -ssltruststorefile <path_to_client_keystore.jks>  
-ssltruststorepassword <your_JKS_password>
```

For example:

```
opsearchtool.cmd enableSSLDbConn -ssltruststorefile c:\keystore\client_keystore.jks  
-ssltruststorepassword JKSpassord
```

- d) Edit the file <SEARCH_HOME>/OPSearch/opsearchtools/openpages_search.properties. Change the port number to the TLS port that your database server is using:
OPSearchTool.DatabasePort = db_secure_port_number.
4. Enable global search.
 - a) Log in to IBM OpenPages with Watson with administrative privileges. Go to the Standard UI.
 - b) Go to **Administration > Global Search** and select **Enable**.

Note: In some rare cases, you might need to pass additional parameters to the Java JRE. If this is the case, you can edit one of the following files to do so.

- For IBM Db2, edit <SEARCH_HOME>/OPSearch/opsearchtools/DatabasePropertyFile_DB2.properties
- For Oracle, edit <SEARCH_HOME>/OPSearch/opsearchtools/DatabasePropertyFile_Oracle.properties

Disabling the TLS database connection between the search server and the database server

If you need to disable the TLS connection between the search server and the database server, follow these steps.

Procedure

1. Disable global search.
 - a) Log in to IBM OpenPages with Watson with administrative privileges. Go to the Standard UI.
 - b) Navigate to **Administration > Global Search** and select **Disable**.
2. Disable TLS on the database server.
3. Start global search.
 - a) Log in to IBM OpenPages with Watson with administrative privileges. Go to the Standard UI.
 - b) Navigate to **Administration > Global Search** and select **Enable**.

Oracle Transparent Data Encryption (TDE)

You can use Oracle Transparent Data Encryption (TDE) to encrypt the OpenPages and Cognos table spaces in the OpenPages database.

This task is optional.

Note: This task is for existing databases. You can also set up TDE when you do a fresh installation. For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

IBM OpenPages with Watson supports the ability to implement TDE, but TDE is an Oracle feature. You need to be familiar with data encryption of Oracle databases and you need to configure and maintain TDE. If you have questions about TDE, refer to the Oracle documentation.

Restriction: OpenPages supports Oracle TDE only for table spaces. Column-based TDE is not supported.

To implement Oracle TDE, you need to complete two main tasks:

1. Configure a keystore. You can do this step at any time after you install OpenPages.

Your database administrator needs to create a keystore. The steps and requirements for keystores are determined by Oracle. IBM is not responsible for the configuration or maintenance of the keystore.
2. Encrypt the table spaces that support encryption.

To implement Oracle TDE on an existing installation of OpenPages, manual database steps are required. These manual steps require database administrator privileges and skills. If you do not have database administration experience, review these manual steps with a database administrator before you set up Oracle TDE.

A table space can be encrypted only when it is initially created. You cannot alter an existing table space to enable encryption. Instead, you drop the table spaces, re-create them with TDE enabled, and then restore the schema.

Note: Oracle does not support encryption on system, undo, or temporary table spaces.

For more information about TDE, refer to the Oracle documentation, such as the [Oracle Database Advance Security Guide \(https://docs.oracle.com/database/121/ASOAG/toc.htm\)](https://docs.oracle.com/database/121/ASOAG/toc.htm).

Prerequisites and process overview

Ensure that your environment meets the prerequisites for Oracle TDE and review the configuration process.

Ensure that your environment meets the following prerequisites:

1. IBM OpenPages with Watson is installed.

2. The Oracle instance is open and accepting connections.
3. All users must be off of the system until all steps in the Oracle TDE configuration process are complete.
4. The database compatibility parameter is set to your version of Oracle:
 - For Oracle 12.2, use 12.2.0
 - For Oracle 18c, use 18.0.0
 - For Oracle 19c, use 19.0.0

Complete the following process to configure Oracle TDE:

1. Configure a software key store. Refer to the [Oracle documentation](#).
2. Encrypt the OpenPages and Cognos table spaces that support encryption:
 - a. Verify the value of the database compatible parameter.
 - b. Do a full backup of the OpenPages schema.
 - c. Do a full backup of the Cognos schema.
 - d. Shut down all OpenPages components.
 - e. Drop the OpenPages and Cognos table spaces.
 - f. Re-create the OpenPages and Cognos table spaces.
 - g. Verify that the table spaces are encrypted.
 - h. Restore the OpenPages schema.
 - i. Restore the Cognos schema.

Encrypting OpenPages and Cognos table spaces

You can encrypt the OpenPages and Cognos table spaces by using Oracle TDE.

Before you begin

Ensure that no users are on the system before you begin.

Do this procedure after you set up the keystore.

Procedure

1. Log on to the OpenPages database instance as the instance owner.
2. Start SQL*Plus.
3. Verify that the database COMPATIBLE parameter is set to the version of Oracle that you are using.

```
select value from GV$SYSTEM_PARAMETER where name = 'compatible';
```

4. Do a full backup of the OpenPages and Cognos databases.

For more information, see [“Backing up the OpenPages database \(Oracle\)”](#) on page 720.
5. Shut down all OpenPages and Cognos components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.
6. Drop all OpenPages and Cognos table spaces.

Do the following steps if your environment meets these criteria:

- OpenPages and Cognos use the same database.
- You are using a standard deployment, where each table space uses a single data file.

If you have multiple data files per table space or if you have customized your deployment in any way, your DBA staff will need to analyze your environment to determine what actions are needed to drop the table spaces.

- a) Determine the list of table spaces.

The default table space names are:

```
AURORA
INDX
AURORA_SNP
AURORA_NL
AURORA_NLI
AURORA_CLOB_DATA
AURORA_DOMAIN_INDX
CRN
```

Run the following query as a DBA user get a list of the existing table spaces:

```
select tablespace_name from dba_tablespaces;
```

- b) Run the following query to collect information about the table spaces.

You will use this information in a later step.

If you use custom table space names, modify the WHERE clause.

```
select dt.tablespace_name,
       df.file_name,
       ceil(df.bytes/1048576)||' M' as file_size
from   DBA_TABLESPACES dt,
       DBA_DATA_FILES df
where  dt.tablespace_name = df.tablespace_name
and    dt.tablespace_name in
       ('AURORA','INDX','AURORA_SNP','AURORA_NL','AURORA_NLI',
        'AURORA_CLOB_DATA','AURORA_DOMAIN_INDX','CRN');
```

Example output:

TABLESPACE_NAME	FILE_NAME	FILE_SIZE
AURORA	/home/oracle/app/oradata/aurora.dbf	640 M
AURORA_CLOB_DATA	/home/oracle/app/oradata/aurora_clob_data.dbf	128 M
AURORA_DOMAIN_INDX	/home/oracle/app/oradata/aurora_domain_indx.dbf	128 M
AURORA_NL	/home/oracle/app/oradata/aurora_nl.dbf	128 M
AURORA_NLI	/home/oracle/app/oradata/aurora_nli.dbf	128 M
AURORA_SNP	/home/oracle/app/oradata/aurora_snp.dbf	256 M
INDX	/home/oracle/app/oradata/indx.dbf	640 M
CRN	/home/oracle/app/oradata/crn.dbf	512 M



Attention: If a table space name appears twice in the output, the database uses more than one data file per table space. In this case, contact your database administrator before you continue.

- c) Delete the database objects.

Log in to SQL*Plus as the OpenPages database user and run the following script:

```
@AuroraDbDelete.sql
```

When the script completes, log out of SQL*Plus.

- d) Drop the table spaces.

Log in to SQL*Plus as a DBA user and run the following commands. If you use custom table space names, use the names that you found in step 6a.

```
drop tablespace AURORA including contents and datafiles;
drop tablespace INDX including contents and datafiles;
drop tablespace AURORA_SNP including contents and datafiles;
drop tablespace AURORA_NL including contents and datafiles;
drop tablespace AURORA_NLI including contents and datafiles;
drop tablespace AURORA_CLOB_DATA including contents and datafiles;
drop tablespace AURORA_DOMAIN_INDX including contents and datafiles;
drop tablespace CRN including contents and datafiles;
```

7. Re-create the table spaces with Oracle TDE configured.

a) Create a .sql file that contains the commands.

Copy the following template into a file. Make the following changes to the file:

- If you use custom table space names, replace the table space names with the names from step 6a.
- Replace the placeholders with the values from step 6b.
- Decide which encryption algorithm to use, and uncomment it from the define encrypt_var=' ' list.
- Save the file.

```
-----  
--          **** Oracle Transparent Data Encryption ****  
-- You can modify the encryption variable below or use one of the provided  
-- options. To use a provided option, uncomment the desired algorithm from  
-- the list below.  
-----  
define encrypt_var=' '  
--define encrypt_var='ENCRYPTION USING '3DES168' DEFAULT STORAGE(ENCRYPT) '  
--define encrypt_var='ENCRYPTION USING 'AES128' DEFAULT STORAGE(ENCRYPT) '  
--define encrypt_var='ENCRYPTION USING 'AES192' DEFAULT STORAGE(ENCRYPT) '  
--define encrypt_var='ENCRYPTION USING 'AES256' DEFAULT STORAGE(ENCRYPT) '  
  
create tablespace AURORA datafile '<file name from query>'  
  size <file size from query> M reuse autoextend on  
  next 128 M &&encrypt_var;  
  
create tablespace INDX datafile '<file name from query>'  
  size <file size from query> M reuse autoextend on  
  next 128 M &&encrypt_var;  
  
create tablespace AURORA_SNP datafile '<file name from query>'  
  size <file size from query> M reuse autoextend on  
  next 128 M &&encrypt_var;  
  
create tablespace AURORA_CLOB_DATA datafile '<file name from query>'  
  size <file size from query> M reuse autoextend on  
  next 128 M &&encrypt_var;  
  
create tablespace AURORA_DOMAIN_INDX datafile '<file name from query>'  
  size <file size from query> M reuse autoextend on  
  next 128 M &&encrypt_var;  
  
create tablespace AURORA_NL nologging datafile '<file name from query>'  
  size <file size from query> M reuse autoextend on  
  next 128 M extent management local uniform size 2 M &&encrypt_var;  
  
create tablespace AURORA_NLI nologging datafile '<file name from query>'  
  size <file size from query> M reuse autoextend on  
  next 128 M extent management local uniform size 2 M &&encrypt_var;  
  
create tablespace CRN datafile '<file name from query>'  
  size <file size from query> M reuse autoextend on  
  next 128 M &&encrypt_var;
```

Sample file:

```
-----  
--          **** Oracle Transparent Data Encryption ****  
-- You can modify the encryption variable below or use one of the provided  
-- options. To use a provided option, uncomment the desired algorithm from  
-- the list below.  
-----  
--define encrypt_var=' '  
--define encrypt_var='ENCRYPTION USING '3DES168' DEFAULT STORAGE(ENCRYPT) '  
define encrypt_var='ENCRYPTION USING 'AES128' DEFAULT STORAGE(ENCRYPT) '  
--define encrypt_var='ENCRYPTION USING 'AES192' DEFAULT STORAGE(ENCRYPT) '  
--define encrypt_var='ENCRYPTION USING 'AES256' DEFAULT STORAGE(ENCRYPT) '  
  
create tablespace AURORA datafile  
  '/home/oracle/app/oradata/aurora.dbf'  
  size 640 M reuse autoextend on next 128 M &&encrypt_var;  
  
create tablespace INDX datafile  
  '/home/oracle/app/oradata/indx.dbf'  
  size 640 M reuse autoextend on next 128 M &&encrypt_var;
```

```

create tablespace AURORA_SNP datafile
'/home/oracle/app/oradata/aurora_snp.dbf'
size 256 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace AURORA_CLOB_DATA datafile
'/home/oracle/app/oradata/aurora_clob_data.dbf'
size 128 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace AURORA_DOMAIN_INDX datafile
'/home/oracle/app/oradata/aurora_domain_indx.dbf'
size 128 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace AURORA_NL nologging datafile
'/home/oracle/app/oradata/aurora_nl.dbf'
size 128 M reuse autoextend on next 128 M extent management
local uniform size 2 M &&encrypt_var;

create tablespace AURORA_NLI nologging datafile
'/home/oracle/app/oradata/aurora_nli.dbf'
size 128 M reuse autoextend on next 128 M extent management
local uniform size 2 M &&encrypt_var;

create tablespace CRN datafile
'/home/oracle/app/oradata/crn.dbf'
size 512 M reuse autoextend on next 128 M &&encrypt_var;

```

b) Log in to SQL*Plus as a DBA user and run the file that you created.

For example, if your file is named `tbasp_create.sql`, log into SQL*Plus as a DBA user and run the following commands:

```

spool tbasp_create.log
@tbasp_create.sql
exit;

```

8. Grant space privileges to the OpenPages and Cognos users on the new table spaces.

Use the following syntax. If you use custom table space names, replace the table space names with the names from step 6a.

```

alter user <openpages db user> quota unlimited on AURORA;
alter user <openpages db user> quota unlimited on INDX;
alter user <openpages db user> quota unlimited on AURORA_NL;
alter user <openpages db user> quota unlimited on AURORA_NLI;
alter user <openpages db user> quota unlimited on AURORA_SNP;
alter user <openpages db user> quota unlimited on AURORA_CLOB_DATA;
alter user <openpages db user> quota unlimited on AURORA_DOMAIN_INDX;
alter user <cognos db user> quota unlimited on CRN;

```

Example:

```

alter user openpage quota unlimited on AURORA;
alter user openpage quota unlimited on INDX;
alter user openpage quota unlimited on AURORA_NL;
alter user openpage quota unlimited on AURORA_NLI;
alter user openpage quota unlimited on AURORA_SNP;
alter user openpage quota unlimited on AURORA_CLOB_DATA;
alter user openpage quota unlimited on AURORA_DOMAIN_INDX;
alter user cognos quota unlimited on CRN;

```

9. Verify that the table spaces are encrypted.

Log in to the OpenPages database as a DBA user and run the following command. If you use custom table space names, replace the table space names in the WHERE clause with the names from step 6a.

```

select tablespace_name, encrypted, status
from dba_tablespaces
where tablespace_name in
('AURORA', 'INDX', 'AURORA_SNP', 'AURORA_NL', 'AURORA_NLI',
'AURORA_CLOB_DATA', 'AURORA_DOMAIN_INDX', 'CRN');

```

Verify that the output is similar to the following text:

TABSPACE_NAME	ENC	STATUS
AURORA	YES	ONLINE
AURORA_CLOB_DATA	YES	ONLINE
AURORA_DOMAIN_INDX	YES	ONLINE
AURORA_NL	YES	ONLINE
AURORA_NLI	YES	ONLINE
AURORA_SNP	YES	ONLINE
INDX	YES	ONLINE
CRN	YES	ONLINE

8 rows selected.

10. Restore the OpenPages schema, and then restore the Cognos schema.

For more information, see [“Import the production data into the test environment”](#) on page 738.

11. Restart all OpenPages and Cognos components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.

Shortening the URL for OpenPages with Watson

You can shorten the IBM OpenPages with Watson application URL. You might shorten the URL to support privacy or to support some mobile uses of the URL. To shorten the URL, change the values for properties in various files.

Before you begin

Before you modify the files that are referenced in this procedure, back up the files.

About this task

In the following example of the default and the shortened URL, the port number of the admin application server is 10108:

Default URL

`http://<server_name>:10108/openpages`

Shortened URL

`http://<server_name>:10108/`

Procedure

1. Log on to the admin application server.
2. Stop the Cognos service and the OpenPages with Watson Framework Model Generator service. For more information, see [“Starting and stopping the Cognos services”](#) on page 849.

3. Edit the following file:

`<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/configDropins/overrides/op-apps.xml`

4. Look for the following lines:

```
<!-- Specify an alternative context-root here for the primary OpenPages web application -->
<!-- <web-ext id="sosa" moduleName="sosa" context-root="/" />-->
```

5. Uncomment the following line:

```
<web-ext id="sosa" moduleName="sosa" context-root="/" />
```

6. Go to the `<OP_HOME>/aurora/conf/` directory.
7. For each of the properties files that are listed in the following table, open the file in a text editor. Change the current value to the new value, and then save the file:

Table 252. Shorten URL, property values		
File name	Current value	New value
aurora.properties	application.url.path=http\:// server_name\:10108/ openpages	application.url.path=http\:// server_name\:10108
Server<#>- server.properties	url.path.openpages=http\:// server_name\:10108/ openpages	url.path.openpages=http\:// server_name\:10108
Server<#>- sosa.properties	application.url.path=http\:// server_name\:10108/ openpages	application.url.path=http\:// server_name\:10108
Server<#>- sosa.properties	application.context=/ openpages	application.context=

8. On the Cognos server, navigate to the following folder: <COGNOS_HOME>/configuration
 - a) Open the OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties file in a text editor or XML editor.
 - b) Change the current value to the new value, and then save the file:

Current value
openpages.application.url=http\://<server_name>\:10108/openpages

New value
openpages.application.url=http\://<server_name>\:10108
9. Restart the OpenPages with Watson application servers. For more information, see [“Starting application servers”](#) on page 841.
10. Start the Cognos service and the Framework Model Generator service. For more information, see [“Starting and stopping the Cognos services”](#) on page 849.
11. After the services are started, log in to OpenPages with Watson.
12. Click  > **System Configuration** > **Settings**.
13. Expand the following folders: **Platform** > **Reporting Schema** > **Object URL Generator** > **Detail Page**. Replace the current value with the new value, and then click **Done**.

Current value
/openpages/view.resource.do

New value
/view.resource.do
14. Re-create the reporting schema. For more information, see [“Creating or recreating the reporting schema \(Standard UI\)”](#) on page 163.

Parameters for cluster members

When working with cluster members, there are values for common parameters. You must enter these parameter values consistently across all of the tasks.

For example, a property or code statement requires the name of the machine on which you are adding the cluster member. That value is represented by the <server_name> parameter. If the name of the machine on which you are adding the cluster member is OP_Host, then you must enter OP_Host whenever you are asked to provide the value for <server_name>.

Table 253. Parameters for cluster members in IBM WebSphere

Parameter	Description
<OP_HOME>	The installation location of the IBM OpenPages with Watson application. By default, <OP_HOME> is c : \IBM\OpenPages on Windows or /opt/IBM/OpenPages on Linux.
<server_name>	The host name of the machine on which you are adding the managed server instance. For example, OP_Host
Server<#>	The number of the managed server you are adding to the cluster. For example, If you currently have one managed server on OP_Host, this parameter value would be Server2.
<OpenPages_default_server_port #>	The value of the op.http.port or op.https.port (if you are using TLS) in the following property file: <OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties For example, 10108

Configuring HTTP compression in OpenPages with Watson

HTTP compression is a technique used to reduce the network bandwidth that is used to transfer files from the server to the client by compressing web content. Compliant web browsers automatically decompress the content before displaying it to users.

For IBM OpenPages with Watson application servers, HTTP compression is installed during the installation process.

By default, HTTP compression is disabled on the application servers to reduce processor usage and improve performance over a local area network (LAN). On systems that use a router or switch to compresses data, you might also want to disable HTTP compression on both the OpenPages with Watson application and Cognos servers in your environment to avoid double compression.

In situations where clients are primarily accessing the servers by using a narrow network bandwidth (such as modems), enable HTTP compression on both application and Cognos servers.

Note: Files that are already compressed, such as image files, PDF, and .zip files will not be compressed to improve performance.

See these topics for details:

- [“Enabling or disabling HTTP compression on OpenPages with Watson Application Servers” on page 818](#)
- [“Enabling or disabling compression on the Cognos Server using Windows IIS” on page 818](#)
- [“Enabling compression on the Cognos Server using Apache Web Server” on page 818](#)
- [“Disabling compression on the Cognos Server using Apache Web Server” on page 819](#)

Enabling or disabling HTTP compression on OpenPages with Watson Application Servers

Follow these steps to enable or disable HTTP compression on IBM OpenPages with Watson application servers via settings in the application user interface.

Note: These steps apply to all OpenPages with Watson application servers in a clustered environment.

Procedure

1. Log on to the OpenPages with Watson application user interface as a user with administrative permissions.
2. Access the Settings page.
3. Set the value in the **Show Hidden Settings** setting to `true`.
4. Expand the **Applications > Common > Configuration > HTTP Compression** folder hierarchy.
5. Click the **Compression Enabled** setting to open its detail page.
6. In the **Value** box, type one of the following values. If the value is set to:
 - `true` – HTTP compression is enabled.
 - `false` - HTTP compression is not enabled.
7. When finished, click **Save**.

The change will take effect immediately.

Enabling or disabling compression on the Cognos Server using Windows IIS

You can enable or disable compression on the Cognos Server using Windows IIS.

Procedure

1. On the Cognos server, click **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the **Connections** pane:
 - a) Expand **Sites > Default Web Site**.
 - b) Select the name of the Cognos folder (for example, cognos).
3. In **Features View**, under **IIS**:
 - a) Double-click **Compression**.
 - b) Do one of the following:
 - To enable compression, select both **Enable dynamic content compression** and **Enable static content compression**.
 - To disable compression, clear both **Enable dynamic content compression** and **Enable static content compression**.
 - c) In the **Actions** pane, click **Apply**.

Enabling compression on the Cognos Server using Apache Web Server

You can enable compression on the Cognos server using Apache Web Server.

HTTP compression can be enabled or disabled on the Apache Web Server for Windows and Linux environments. The Apache source package includes the `mod_deflate` module, which provides for the compression of web content. By default, this module is not enabled.

Procedure

1. On the Cognos server, navigate to the `<Apache_Home>|conf` directory.

Where: `<Apache_Home>` is the installation location of the Apache Web Server. For example, for Windows, a directory structure might be `C:\Program Files (x86)\Apache2.2` and for Linux, the directory structure might be `/opt/pware/`.

2. Navigate to the `httpd.conf` file and do the following:

- a) Make a backup copy of the file before modifying it.
- b) Open the `httpd.conf` file in a text editor of your choice.

3. In the `httpd.conf` file, load the `mod_deflate` module as follows.

- a) Verify that the following statement is present at the beginning of the file:

```
LoadModule deflate_module modules/mod_deflate.so
```

- b) If the `mod_deflate` module statement in Step 3a is commented out (has a `#` (number sign) at the beginning of the line), then remove the `#` (number sign) so the compression module will be loaded.

4. At the bottom of the `httpd.conf` file, add the following block of configuration code to enable compression:

```
<IfModule deflate_module>
SetOutputFilter DEFLATE
<IfModule setenvif_module>
# Netscape 4.x has some problems
BrowserMatch ^Mozilla/4 gzip-only-text/html
# Netscape 4.06-4.08 have some more problems
BrowserMatch ^Mozilla/4\.[0678] no-gzip
# MSIE masquerades as Netscape, but it is fine
BrowserMatch \bMSIE!no-gzip!gzip-only-text/html
# Don't compress already-compressed files
SetEnvIfNoCase Request_URI \.(?:gif|jpe?g|png)$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \.pdf$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \.(?:exe|t?gz|zip|bz2|sit|rar)$ no-gzip dont-vary
# Make sure proxies don't deliver the wrong content
Header append Vary User-Agent env=!dont-vary
</IfModule>
</IfModule>
```

5. Depending on your environment, do one of the following to restart the Apache Web Server.

- For Windows:
 - Click **Start > Windows Administrative Tools > Services**.
 - Right-click the Apache`<version>` service and select **Restart**.
- For Linux:
 - Log on to the Cognos server as the root user.
 - Navigate to the `<Apache_Home>/bin` directory.
 - Enter the following command to stop the server:

```
./apachectl stop
```

- Type the following command to re-start the server:

```
./apachectl start
```

Disabling compression on the Cognos Server using Apache Web Server

You can disable compression on the Cognos server using Apache Web Server.

Note: This information applies to Windows and Linux environments.

Procedure

1. On the Cognos server, navigate to the `<Apache_Home>|conf` directory.

Where: `<Apache_Home>` is the installation location of the Apache Web Server. For example, for Windows, a directory structure might be `C:\Program Files (x86)\Apache2.2` and for Linux, the directory structure might be `/opt/pware/`.

2. Navigate to the `httpd.conf` file and do the following:

- a) Make a backup copy of the file before modifying it.
- b) Open the `httpd.conf` file in a text editor of your choice.

3. From the bottom of the `httpd.conf` file, remove the following block of configuration code to disable compression:

```
<IfModule deflate_module>
SetOutputFilter DEFLATE
<IfModule setenvif_module>
# Netscape 4.x has some problems
BrowserMatch ^Mozilla/4 gzip-only-text/html
# Netscape 4.06-4.08 have some more problems
BrowserMatch ^Mozilla/4\.[0678] no-gzip
# MSIE masquerades as Netscape, but it is fine
BrowserMatch \bMSIE[ ] !no-gzip !gzip-only-text/html
# Don't compress already-compressed files
SetEnvIfNoCase Request_URI \.(?:gif|jpe?g|png)$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \.pdf$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \.(?:exe|t?gz|zip|bz2|sit|rar)$ no-gzip dont-vary
# Make sure proxies don't deliver the wrong content
Header append Vary User-Agent env=!dont-vary
</IfModule>
</IfModule>
```

4. When finished, save the file.
5. Depending on your environment, do one of the following to restart the Apache Web Server.

- For Windows:
 - Click **Start > Windows Administrative Tools > Services**.
 - Right-click the Apache`<version>` service and select **Restart**.
- For Linux:
 - Log on to the Cognos server as the root user.
 - Navigate to the `<Apache_Home>/bin` directory.
 - Enter the following command to stop the server:

```
./apachectl stop
```

- Type the following command to re-start the server:

```
./apachectl start
```

Factors that affect performance of activity and grid views

When you design activity or grid views, keep in mind the following factors that can affect the performance.

Number of paths

The more paths in the activity view the more work the application must do to traverse those paths and provide a result. The more paths that you specify the longer it takes to provide a result.

Depth of paths

Each object type in the path results in an incremental increase in the work that is required to traverse the path. The deeper a certain path is, the longer it takes to provide a result for that path.

Number of child objects per top-level object

The ratio of top-level objects to child objects determines how much work the application must do to gather the total result set. The more child objects per top-level object, the longer it takes to provide a result.

Security rules (RLS/FLS)

Security rules are processed in the context of the individual instance of an object. The mere inclusion of even a simple security rule increases the work that is required in the application to obtain a result set. As the complexity of the security rule increases, the time it takes to provide a result also increases.

Server tuning settings

To avoid time-out issues when using IBM OpenPages with Watson, you must configure the servers and the database.

Important: All tuning settings assume a maximum of 1000 concurrent users per node.

Changing JVM options on application servers

You can adjust the Java Virtual Machine (JVM) options on the IBM OpenPages with Watson application servers.

About this task

The IBM OpenPages with Watson installation process configures the JVM when you install, upgrade, or migrate OpenPages. You can view the default JVM options in the following file: `<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/jvm.options`. In most cases, you do not need to change the defaults. If you do need to change them, use an override file.

Procedure

1. Log on to the application server.
2. Edit the following file: `<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/configDropins/overrides/jvm.options`
If the file does not exist, create it by using a text editor.
3. Type the JVM options that you want to change. Type each option on a new line.
For example, the following lines set the initial heap size to 1 GB and the maximum heap size to 4 GB.

```
-Xms1g  
-Xmx4g
```

Note: This example shows the options that OpenPages uses by default.

For more information, see the [WebSphere Liberty documentation](#).

4. If this is a load-balanced environment, repeat this procedure on each application server in the load-balanced environment.
5. Restart all OpenPages with Watson services.
For more information, see [“Starting application servers” on page 841](#).

Configuring the reporting server

Configure the reporting server to avoid time-out issues.

About this task

The reporting server is a component of Cognos Analytics. You configure the reporting server using IBM Cognos Configuration and IBM Cognos Administration.

Procedure

1. Log on to the Cognos server as a user with administrative permissions.
2. Go to the <COGNOS_Home>\bin64 directory.
3. Double-click the cogconfigw.exe file to start IBM Cognos Configuration, the Cognos Analytics configuration tool.
4. In the **Explorer** pane, expand **IBM Cognos services**, and click the **IBM Cognos** service.
5. In the properties pane, set the **Maximum memory for Tomcat in MB** property to **1024**.
6. From the **File** menu, click **Save** to save the updated Cognos Analytics configuration.
7. Go to IBM Cognos Administration, click the **Configuration** tab, and then click **Dispatchers and Services**.
8. Click the dispatcher that is used by your Cognos Analytics installation, and in the list of services find **ReportService**.
9. In the **Actions** column, click the **Set properties - ReportService** icon associated with the report service.
10. In the report service properties page, click the **Settings** tab, and specify the following settings.
Note: To filter on the tuning settings in the list, under **Category**, click **Tuning**.
 - Set the **Number of low affinity connections for the report service during non-peak period** to **8**.
 - Set the **Maximum number of processes for the report service during non-peak period** to **8**.
 - Set the **Number of low affinity connections for the report service during peak period** to **8**.
 - Set the **Maximum number of processes for the report service during peak period** to **12**.
11. Click **OK** to apply the settings.

Configuring the database (Db2)

Configure the IBM Db2 database to avoid time-out issues.

Procedure

1. Open the database console running as a Db2 administrator.
2. Set the tuning parameters by using the following command:

```
db2 update db cfg for <DATABASE_NAME> using <VARIABLE> <VALUE>
```

For example, db2 update db cfg for <DATABASE_NAME> using SELF_TUNING_MEM ON

The following table describes the tuning parameter settings to use. Values shown in brackets are informational when the parameter is set to AUTOMATIC. This enables Db2 to control the parameter and reflects the current setting.

Table 254. Database tuning parameters		
Parameter	Description	Value (default)
SELF_TUNING_MEM	Self tuning memory	ON
DATABASE_MEMORY	Size of database shared memory (4KB)	AUTOMATIC (2683751)
DB_MEM_THRESH	Database memory threshold	10
LOCKLIST	Max storage for lock list (4KB)	AUTOMATIC (82212)
MAXLOCKS	Percentage of lock lists per application	AUTOMATIC (97)
PCKCACHESZ	Package cache size (4KB)	AUTOMATIC (419456)

Table 254. Database tuning parameters (continued)		
Parameter	Description	Value (default)
SHEAPTHRES_SHR	Sort heap threshold for shared sorts (4KB)	AUTOMATIC (63309)
SORTHEAP	Sort list heap (4KB)	AUTOMATIC (12661)
DBHEAP	Database heap (4KB)	AUTOMATIC (5405)
CATALOGCACHE_SZ	Catalog cache size (4KB)	4000
LOGBUFSZ	Log buffer size (4KB)	2560
UTIL_HEAP_SZ	Utilities heap size (4KB)	306174
STMT_HEAP	SQL statement heap (4KB)	AUTOMATIC (51200)
APPLHEAPSZ	Default application heap (4KB)	25600
APPL_MEMORY	Application Memory Size (4KB)	AUTOMATIC (40000)
STAT_HEAP_SZ	Statistics heap size (4KB)	AUTOMATIC (4384)
DLCHKTIME	Interval for checking deadlock (ms)	10000
LOCKTIMEOUT	Lock timeout (sec)	-1
CHNGPGS_THRESH	Changed pages threshold	80
NUM_IOCLEANERS	Number of asynchronous page cleaners	AUTOMATIC (10)
NUM_IOSERVERS	Number of I/O servers	AUTOMATIC (44)
SEQDETECT	Sequential detect flag	YES
DFT_PREFETCH_SZ	Default prefetch size (pages)	AUTOMATIC
TRACKMOD	Track modified pages	NO
	Default number of containers	1
DFT_EXTENT_SZ	Default tablespace extent size (pages)	32
MAXAPPLS	Max number of active applications	300
AVG_APPLS	Average number of active applications	10
MAXFILOP	Max DB files open per application	61440

3. Save your changes.
4. Validate the changes using the following command:

```
db2 get db cfg for <DATABASE_NAME>
```

Improve the performance of OpenPages application functions on a Db2 server

You can improve the performance of IBM OpenPages with Watson application functions by collecting performance statistics for the IBM Db2 server, and by rebinding OpenPages pl/sql packages.

Examples of application functions include importing instance data using FastMap, importing metadata using ObjectManager, and updating the OpenPages repository using SCOR rules.

Up-to-date statistics are necessary for the proper performance of OpenPages applications that use a Db2 server. You can use a script to force the Db2 server to collect statistics, and by default, rebind all OpenPages pl/sql packages. The script requires all OpenPages application services to stop before it runs. For details on stopping servers, see [Chapter 24, “Starting and stopping servers,” on page 841](#).

You run the script from the primary OpenPages application server. You do not need to run this script from all cluster member servers, but you must stop all cluster member services before running the script to rebind OpenPages pl/sql packages.

If a database is still running, you see the error SQL1026N. If this happens, verify that OpenPages services are not running, and disconnect all active connections to the database before continuing.

You can run the script on Microsoft Windows and Linux.

1. For Windows users only, type the following command in a command prompt window to initialize the Db2 command line processor (CLP):

```
db2cmd
```

2. Browse to the `<OP_HOME>|aurora|bin|db2stats` directory.
3. Run the following script:

- On Windows: `CollectSchemaStatistics.bat [-n] [-i]`
- On Linux: `CollectSchemaStatistics.sh [-n] [-i]`

Use these parameters as required:

- `[-n]` to skip rebinding of database packages.
- `[-i]` to run the script in interactive mode.

The script execution time varies depending on OpenPages application usage.

You can schedule this script to run by using a task scheduler, cronjob, or similar utility. The suggested schedule to use is as follows:

- Schedule the script to run daily without rebinding of OpenPages pl/sql packages.
- Schedule the script to run once a week with rebinding of OpenPages pl/sql packages.

Installing tools and utilities (IBM OpenPages with Watson)

Tools and utilities, such as ObjectManager, are available on the application servers. But you can also install them on remote systems, such as your laptop, and run them remotely.

Before you begin

The computer where you install the tools and utilities must meet the following requirements:

- IBM SDK, Java Technology Edition 8 or Java Runtime Environment (JRE) 8 is installed.
- `JAVA_HOME` is defined.
- The computer must be able to communicate with the OpenPages application server.

About this task

Do this task if you want to run any of the following tools from a remote system:

- ObjectManager: See Chapter 27, “The ObjectManager tool,” on page 881.
- Update Password Encryption Algorithm (UPEA): See [“Updating the password encryption algorithm” on page 99.](#)
- chng-sys-password.sh | .bat: See [“Changing the OPSysSystem password” on page 773.](#)
- RpsRpf.sh | .bat: A command line tool for creating the reporting schema and generating the reporting framework. See [“Generating the reporting schema and framework from a command line” on page 164.](#)
- Notification Manager: See [Appendix A, “The Notification Manager,” on page 1075.](#)

For information about client side tool logs, see [“Client tool log files” on page 831.](#)

If you're using IBM OpenPages for IBM Cloud Pak for Data, see [“Installing tools and utilities in Cloud Pak for Data” on page 44.](#)

Procedure

1. Get the installation package.

Go to the `/OP_<version>_Main/OP_<version>_Tools` directory on the installation media.
Download the `openpages-tools-client.zip` file.

2. Extract the `openpages-tools-client.zip` file to a new directory.
3. Go to the `openpages-tools-client/bin` directory.
4. Open the `openpages-tools-client.properties` file in a text editor.
5. Update the value of the `rest.url.path` property.
Type the base URL of the public REST API on the application server.

```
https\://<host>\:<port>/grc/api
```

Replace `<host>` and `<port>` with the hostname and port of the OpenPages application server.

6. By default, the application server's TLS (SSL) certificate is checked for validity when you run tools such as ObjectManager. To change this behavior, update the `insecure.skip.tls.verify` property.
For more information, see [“Tools properties and parameters ” on page 1085.](#)
7. Save and close the file.

Results

You can now run the tools by using the scripts and properties files in the `openpages-tools-client/bin` directory.

Using log files

The IBM OpenPages with Watson application writes error and other messaging information to a standard set of log files. You can use these log files to troubleshoot reporting and general user errors that may occur.

Configuring extended access logging on WebSphere Liberty

You can configure extended access logging on WebSphere Liberty.

Procedure

1. Log on to the application server.
2. Edit the following file:
`<OP_HOME>/wlp-user/servers/<server_name>/configDropins/overrides/op-apps.xml`
3. Add the following lines to the file.

```
<httpAccessLogging id="accessLogging"/>
<httpEndpoint id="defaultHttpEndpoint" accessLoggingRef="accessLogging"/>
```

For more information about logging options, see the WebSphere Liberty [documentation](#).

4. Repeat these steps on each application server.

Results

The log file is `<OP_HOME>/wlp-user/servers/<server_name>/logs/http_access.log`.

Collect log files and diagnostic data

You can use the LogCollector tool to collect log files and diagnostic data from the IBM OpenPages with Watson environment and from OpenPages databases.

Note: If you're using IBM OpenPages for IBM Cloud Pak for Data, use the IBM Cloud Pak for Data web client to collect log files and diagnostic data.

The LogCollector tool collects log files and diagnostic data on an application server.

In a horizontal cluster environment, run the tool on each application server in your environment.

In a vertical cluster, with multiple application servers that are installed on the same machine, the tool gathers logs from all servers. The tool gathers logs from reporting servers only when they are installed on the same machine as one of the application servers. If the search server is also installed on the same machine, for example in a development environment, the tool also collects the search server logs.

The LogCollector tool is in the `<OP_HOME>/bin` directory.

The tool uses the following command options:

Note: For all command options, the long name command option uses two hyphens (--), whereas the short name uses only 1 hyphen (-).

--configuration or -c

Use to specify a configuration file path.

If you do not include this option, the default is `LogCollector.xml`.

Using --configuration or -c is optional.

--database or -d

Use to collect log and diagnostic data from only the database.

--file or -f

Use to collect only log and diagnostic files.

--location or -l

Use to specify the path where the output file will be stored.

If you specify both -l and -t, use -t for the file name and -l for the path. For example, -l /temp -t test.zip creates /temp/test.zip.

If you don't specify -l, the default location is the directory from which you run the command.

--property or -p

Use to set property values.

Using --property or -p is optional. If you do not include this option, the utility automatically retrieves these values from the local configuration. You need to supply these property values only if you want to override the default behavior.

You must include -p for each property that you use. For example, -p DB_OP_USER <username> -p DB_OP_PASSWORD <password>. The properties that you can use are:

Property	Description
DB_OP_USER	The OpenPages database username

Property	Description
DB_OP_PASSWORD	The OpenPages database user's password If the password contains special characters, surround the password in quotation marks: • Windows: "password" • Linux: 'password' For more information, see “Special characters in passwords” on page xxxvi.
DB_TYPE	The database type. This value can be db2 or oracle.
DB_URL	The database JDBC URL.

--target or -t

Use to specify a target package file.

If you do not include this option, the default is LogCollector_<timestamp>.zip. Using --target or -t is optional.

--help or -h

Use to display command help.

Example: Getting all information

1. Log in as the Super Administrator user.
2. Open a command line window.
3. Go to the <OP_HOME>/bin directory. For example, on Microsoft Windows operating systems, go to C:\IBM\OpenPages\bin. On Linux operating systems, go to /opt/IBM/OpenPages/bin.
4. Enter the following command:

On Microsoft Windows operating systems: LogCollector.cmd

On Linux operating systems: ./LogCollector.sh

The tool generates a package file that is named LogCollector_<timestamp>.zip in the <OP_HOME>/bin.

Example: Specifying a target package file

1. Log in as the Super Administrator user.
2. Open a command line window.
3. Go to the <OP_HOME>/bin directory. For example, on Microsoft Windows operating systems, go to C:\IBM\OpenPages\bin. On Linux operating systems, go to /opt/IBM/OpenPages/bin.
4. Enter the following command:

On Microsoft Windows operating systems: LogCollector.cmd -t LogCollector.zip

On Linux operating systems: ./LogCollector.sh -t LogCollector.zip

The tool generates a package file that is named LogCollector.zip in the <OP_HOME>/bin directory.

Example: Getting information for the database

1. Log in as the Super Administrator user.
2. Open a command line window.
3. Go to the <OP_HOME>/bin directory. For example, on Microsoft Windows operating systems, go to C:\IBM\OpenPages\bin. On Linux operating systems, go to /opt/IBM/OpenPages/bin.

4. Enter the following command:

On Microsoft Windows operating systems: `LogCollector.cmd -d`

On Linux operating systems: `LogCollector.sh -d`

The tool generates a package file that is named `LogCollector_<timestamp>.zip` in the `<OP_HOME>/bin`.

Example: Getting information from a database and specifying the connection information

This example shows how to use the `-d` and `-p` options. Use `-p` when you want to override the database connection information that is configured on your local server.

1. Log in as the Super Administrator user.
2. Open a command line window.
3. Go to the `<OP_HOME>/bin` directory. For example, on Microsoft Windows operating systems, go to `C:\IBM\OpenPages\bin`. On Linux operating systems, go to `/opt/IBM/OpenPages/bin`.
4. Enter the following command:

On Microsoft Windows operating systems:

```
LogCollector.cmd -d -p DB_TYPE db2 -p DB_URL jdbc:db2://localhost:50000/OPX
-p DB_OP_USER openpage -p DB_OP_PASSWORD "password"
```

On Linux operating systems:

```
./LogCollector.sh -d -p DB_TYPE db2 -p DB_URL jdbc:db2://localhost:50000/OPX
-p DB_OP_USER openpage -p DB_OP_PASSWORD 'password'
```

The tool generates a package file that is named `LogCollector_<timestamp>.zip` in the `<OP_HOME>/bin`.

OpenPages with Watson Standard Application Server log files (8.2.0.3 and earlier)

The IBM OpenPages with Watson Standard Application Server log files are located in `<OP_Home>|aurora|logs`. File names vary depending on your environment.

Log file names on application servers

Log file names on the application servers contain information to understand what occurs during startup and application usage.

Where `<server_name>` is the name of the IBM OpenPages with Watson application server.

`<#>` represents the number of the server (for example, `opappServer1`).

Table 255. Application server log files	
This log file...	Contains this type of information...
<code><server_name>Server<#>-startup.log</code>	Messages written during initialization of the OpenPages with Watson application caches on the OpenPages server.
<code><server_name>Server<#>-aurora.log</code>	Errors, exceptions, and informational messages written during OpenPages with Watson application use.

Table 255. Application server log files (continued)	
This log file...	Contains this type of information...
<server_name>Server<#>-auroratools.log	Errors, exceptions, and informational messages written during OpenPages with Watson application use that are invoked by OpenPages utilities. For example, Notification Manager, Object Manager, etc.

Changing the size and number of backups of the aurora log file

An IBM OpenPages with Watson administrator can control the maximum size of the aurora log file and how many backup files are created when the file reaches its maximum size.

About this task

The default maximum file size of the `auroralogging.properties` is 1024 KB. The default number of backups is 10.

Procedure

1. Log on to the OpenPages application server.
2. Go to `<OP_HOME>|aurora|conf` where `<OP_HOME>` is the OpenPages installation location.
By default, `<OP_HOME>` is `c:\IBM\OpenPages` on Windows or `/opt/IBM/OpenPages` on Linux.
3. Back up the `auroralogging.properties` file.
4. Open the `auroralogging.properties` file with a text editor.
5. To change the maximum file size of the `auroralogging.properties` file, modify the `log4j.appender.FILE.MaxFileSize` property.

For example, to change the maximum file size to 5120 KB, change the property to the following:

```
log4j.appender.FILE.MaxFileSize=5120KB
```

6. To change the number of backups of the `auroralogging.properties` file, modify the `log4j.appender.FILE.MaxBackupIndex` property.

For example, to change the number of backups to 20, change the property to the following:

```
log4j.appender.FILE.MaxBackupIndex=20
```

Enabling trace logging

You can enable trace logs for different features within IBM OpenPages with Watson to help diagnose issues that you might run into.

About this task

Trace logging generates a large amount of data on the application server. Enable trace logging only during testing and when other users are not on the system. Make sure to disable trace logging before users access the server again.

When trace logging is enabled, separate log files are created in the `<OP_HOME>/aurora/logs/debug` directory. These log files have a suffix that indicates the log type, for example `<server_name>-workflow.log`, `<server_name>-sdk.log`, and so on.

Generally, trace logs contain the following information:

- Enter and exit messages for relevant API calls

- Timings for each method
- Targeted debug logging

The following trace logs are available:

- Trigger Logger – Logs trigger evaluations and executions.
- Workflow Logger – Logs all workflow API calls and action evaluations.
- Calculation Logger – Logs all calculations.
- Cognos Integration Logger – Logs computed fields, reporting fragments, and connections to Cognos Analytics from OpenPages.
- SDK Logger – Logs all SDK API calls.
- Cache Logger – Logs cache loading at startup and logs updates that occur over time.
- Persistence Logger – Logs database access.
- Custom REST Logger – Logs access to custom rest endpoints.

In 8.2.0.1 and later, you can also use the Login Logger to log all single sign-on authentication events. The log file is named `<OP_HOME>/aurora/logs/debug/<server_name>-auth.log`.

Procedure

1. Log on to the OpenPages application server.
2. Go to the `<OP_HOME>/aurora/conf` directory.
3. Back up the `auroralogging.properties` file.
4. Open the `auroralogging.properties` file with a text editor.
5. To use a trace logger, remove the `#` at the beginning of the line.

In this example, the Workflow Logger is enabled:

```
log4j.logger.com.ibm.openpages.api.service.ejb.workflow.impl=TRACE#com.openpages.aurora.common.logging.Log4jEventLoggerLevel, workflow
```

6. To enable logging for single sign-on authentication events, do the following steps:

Note: This feature is supported in 8.2.0.1 and later.

- a) Uncomment each line in the `# login logger` section:

```
# login logger
log4j.logger.com.openpages.apps.session.OPAppSession=TRACE#com.openpages.aurora.common.logging.Log4jEventLoggerLevel, auth
log4j.logger.com.openpages.aurora.service.security.SecurityUtil=TRACE#com.openpages.aurora.common.logging.Log4jEventLoggerLevel, auth
log4j.logger.com.openpages.singlesignon=TRACE#com.openpages.aurora.common.logging.Log4jEventLoggerLevel, auth
log4j.logger.com.openpages.apps.common.authentication=TRACE#com.openpages.aurora.common.logging.Log4jEventLoggerLevel, auth
log4j.logger.com.ibm.openpages.app.logon=TRACE#com.openpages.aurora.common.logging.Log4jEventLoggerLevel, auth
```

- b) To increase the logging level from DEBUG to TRACE, do the following steps.



Attention: When the logging level is set to TRACE, the log can contain Personal Information (PI) such as usernames and emails.

- i) Locate the following line:

```
#TRACE level may contain sensitive information such as user names
log4j.appender.auth.Threshold=DEBUG#com.openpages.aurora.common.logging.Log4jEventLoggerLevel
```


ii) Change Threshold=DEBUG to Threshold=TRACE:

```
#TRACE level may contain sensitive information such as user names
log4j.appender.auth.Threshold=TRACE#com.openpages.aurora.common.logging.Log4jEventLoggerLevel
```

7. Save your changes and close the file.

8. When you finish debugging, disable the trace loggers.

a) Restore the backup of the auroralogging.properties file. Or, type a # at the start of the lines.

b) Restart the OpenPages application server.

OpenPages with Watson standard log files (8.2.0.4 and later)

These log files use the Apache Log4j 2 framework. For more information on Apache Log4j 2, see the [Apache Log4j 2 documentation](#).

Log files on application servers

Log files on the application servers contain information to understand what occurs during startup and application usage.

The IBM OpenPages with Watson standard Application Server log files are located in <OP_Home>/aurora/logs and <OP_Home>/aurora/logs/debug. File names vary depending on your environment.

Where <server_name> is the name of the IBM OpenPages with Watson application server.

<#> represents the number of the server (for example, opappServer1).

Table 256. Application server log files	
This log file...	Contains this type of information...
<server_name>Server<#>-startup.log	Messages written during initialization of the OpenPages with Watson application caches on the OpenPages server.
<server_name>Server<#>-aurora.log	Errors, exceptions, and informational messages written during OpenPages with Watson application use.
<server_name>Server<#>-reportingframework.log	Logs for the reporting framework

Client tool log files

Client tools are tools that you can run from a remote system. Log files for client tools contain information about errors and exceptions, and also contain informational messages written by OpenPages client tools, such as Notification Manager and ObjectManager.

The IBM OpenPages with Watson client tool log files are located in <OP_HOME>/bin/logs where <OP_HOME> is the directory where you set up the client tools.

Table 257. Client tool log files	
This log file...	Contains this type of information...
<OP_HOME>/bin/logs/openpages-tools-client.log	Messages written for all OpenPages client tools including ObjectManager.
<OP_HOME>/bin/logs/ObjectManager.log	Messages written for ObjectManager client commands only.

For more information about client side tools, see [“Installing tools and utilities \(IBM OpenPages with Watson\)”](#) on page 824.

Changing the size and number of backups of the aurora log file

An IBM OpenPages with Watson administrator can control the maximum size of the aurora log file and how many backup files are created when the file reaches its maximum size.

About this task

The default maximum file size of the `auroralogging.properties` is 1024 KB. The default number of backups is 10.

Procedure

1. Log on to the OpenPages application server.
2. Go to `<OP_HOME>|aurora|conf` where `<OP_HOME>` is the OpenPages installation location.
By default, `<OP_HOME>` is `c:\IBM\OpenPages` on Windows or `/opt/IBM/OpenPages` on Linux.
3. Back up the `auroralogging.properties` file.
4. Open the `auroralogging.properties` file with a text editor.
5. To change the maximum file size of the `auroralogging.properties` file, modify the `appender.FILE.policies.size.size` property.

For example, to change the maximum file size to 5120 KB for all appenders, change the property to the following:

```
appender.FILE.policies.size.size = 5120KB
```

You can define the maximum file size for each appender using the following format:

```
appender.<appender_name>.policies.size.size = <file_size>
```

6. To change the number of backups of the `auroralogging.properties` file, modify the `appender.FILE.strategy.max` property.

For example, to change the number of backups to 20 for all appenders, change the property to the following:

```
appender.FILE.strategy.max = 20
```

You can define the number of backups for each appender using the following format:

```
appender.<appender_name>.strategy.max = <number_of_backups>
```

Enabling trace logging

You can enable trace logs for different features within IBM OpenPages with Watson to help diagnose issues that you might run into.

About this task

Trace logging generates a large amount of data on the application server. Enable trace logging only during testing and when other users are not on the system. Make sure to disable trace logging before users access the server again.

When trace logging is enabled, separate log files are created in the `<OP_HOME>/aurora/logs/debug` directory. These log files have a suffix that indicates the log type, for example `<server_name>-workflow.log`, `<server_name>-sdk.log`, and so on.

Generally, trace logs contain the following information:

- Enter and exit messages for relevant API calls
- Timings for each method
- Targeted debug logging

The following trace logs are available:

<i>Table 258. Loggers and associated appenders</i>			
Loggers	Appenders	Log file location	Description
triggers	trigger	<OP-HOME>/aurora/ logs/debug/ <server_name>- trigger<log_suffix>.log	Logs trigger evaluations and executions
workflow	workflow	<OP-HOME>/aurora/ logs/debug/ <server_name>- workflow<log_suffix>.log	Logs all workflow API calls and action evaluations
calculation	calculation	<OP-HOME>/aurora/ logs/debug/ <server_name>- calculation<log_suffix>.log	Logs all calculations
cognos	cognos	<OP-HOME>/aurora/ logs/debug/ <server_name>- cognos<log_suffix>.log	Logs computed fields, reporting fragments, and connections to Cognos Analytics from OpenPages
sdk	sdk	<OP-HOME>/aurora/ logs/debug/ <server_name>- sdk<log_suffix>.log	Logs all SDK API calls
sdkcache	cache	<OP-HOME>/aurora/ logs/debug/ <server_name>- cache<log_suffix>.log	Logs caching infrastructure messages
auroracache	cache	<OP-HOME>/aurora/ logs/debug/ <server_name>- cache<log_suffix>.log	Logs application-specific cache messages
persistence	persistence	<OP-HOME>/aurora/ logs/debug/ <server_name>- persistence<log_suffix>.log	Logs database access
rest	rest	<OP-HOME>/aurora/ logs/debug/ <server_name>- rest<log_suffix>.log	Logs access to custom rest endpoints

Table 258. Loggers and associated appenders (continued)

Loggers	Appenders	Log file location	Description
webdav	webdav	<OP-HOME>/aurora/ logs/debug/ <server_name>- webdav<log_suffix> .log	Logs trace information for the MS Office integration
dataaccess	dataaccess	<OP-HOME>/aurora/ logs/ <server_name>- dataaccess<log_suf fix>.log	Log for all Create/ Read/Update/Delete operations in the DB, along with associated accessed data
reportingframework	reportingframework	<OP-HOME>/aurora/ logs/ <server_name>- reportingframework <log_suffix>.log	Logs debug information for the reporting framework generation
watson	watson	<OP-HOME>/aurora/ logs/debug/ <server_name>- watson<log_suffix> .log	Logs debugging information for the integration with Watson Language Translation
opappsession	auth	<OP-HOME>/aurora/ logs/debug/ <server_name>- auth<log_suffix>.l og	Tracks log in and log out for a user on the OpenPages application session
securityutil	auth	<OP-HOME>/aurora/ logs/debug/ <server_name>- auth<log_suffix>.l og	Tracks log in and authentication to OpenPages. Also logs if the user is locked out, disabled by an admin, or SAM is blocking their login.
sso	auth	<OP-HOME>/aurora/ logs/debug/ <server_name>- auth<log_suffix>.l og	Logs Single Sign On (SSO) authentication for OpenPages
logon	auth	<OP-HOME>/aurora/ logs/debug/ <server_name>- auth<log_suffix>.l og	Logs OpenPages log on and log off for both Form-Based and SSO authentication. Also logs if the user is locked out, disabled by an admin, or SAM is blocking their log in, and logs initial redirects after user log in is successful or unsuccessful. Applies to the Task Focused UI.

Table 258. Loggers and associated appenders (continued)

Loggers	Appenders	Log file location	Description
authentication	auth	<OP-HOME>/aurora/ logs/debug/ <server_name>- auth<log_suffix>.log	Same as the logon logger but it applies to the Standard UI
feeds	feeds	<OP-HOME>/aurora/ logs/debug/ <server_name>- feeds<log_suffix>.log	Logs third party feeds, such as Thomson Reuters or Wolters Kluwer, and Watson Knowledge Catalog integrations
quartz	scheduler	<OP-HOME>/aurora/ logs/debug/ <server_name>- scheduler<log_suff ix>.log	Logs information for debugging the 3rd party component, Quartz, used by the OP Scheduling service
scheduler	scheduler	<OP-HOME>/aurora/ logs/debug/ <server_name>- scheduler<log_suff ix>.log	Logs information for debugging the OP Scheduler Service

Procedure

1. Log on to the OpenPages application server.
2. Go to the <OP_HOME>/aurora/conf directory.
3. Back up the auroralogging.properties file.
4. Open the auroralogging.properties file with a text editor.
5. To use a trace logger, add the name of the logger to the loggers = entry near the top of the file, and add its associated appender to the appenders = entry.
For example, to enable workflows, add the logger and appender as follows:

```
appenders = CONSOLE, FILE, startup, reportingframework, workflow
loggers = startup, reportingframework, rps, workflow
```

6. To enable logging for single sign-on authentication events, add the opappsession, securityutil, sso, authentication, logon loggers to the loggers = entry along with the associated appender auth to appenders = entry as follows:

```
appenders = CONSOLE, FILE, startup, reportingframework, auth
loggers = startup, reportingframework, rps, opappsession, securityutil, sso, authentication,
logon
```

- a) To increase the logging level from DEBUG to TRACE, do the following steps.



Attention: When the logging level is set to TRACE, the log can contain Personal Information (PI) such as user names and emails.

- i) Locate the following lines:

```
#TRACE level may contain sensitive information such as user names
appender.auth.filter.threshold.type = ThresholdFilter
appender.auth.filter.threshold.level = DEBUG
```

- ii) Change `appender.auth.filter.threshold.level = DEBUG` to `appender.auth.filter.threshold.level = TRACE`.

7. Save your changes and close the file.

8. When you finish debugging, disable the loggers.

Restore the back up of the `auroralogging.properties` file. Or, remove the logger and appender names from the `loggers =` and `appenders =` entries in the properties file.

Logging configuration will be automatically refreshed in 60 seconds without requiring a server restart.

Troubleshooting browser issues

If you have a problem with a browser, review these topics to determine whether a solution is available.

Optimizing application performance in Microsoft Edge browsers

To optimize the performance of the IBM OpenPages with Watson application in Microsoft Edge browsers, you can increase the disk space setting for temporary internet files to 200 MB on client machines.

Procedure

1. From the **Control Panel**, open **Internet Options**.
2. Click the **General** tab.
3. Under **Browsing history**, click **Settings**.
4. In the **Temporary Internet Files and History Settings** box, enter 200 in the disk space box.
5. Restart the browser.

Setting a session inactivity timeout value

The IBM OpenPages with Watson system will timeout a user session after a set period of browser inactivity.

You can modify the value of the inactivity timeout period for the application server and for the reporting server. In general, the timeout period for the IBM Cognos reporting server should be set to a value greater than the application server timeout period.

In this example, the IBM Cognos server inactivity timeout value is set to 90 minutes, and the application server timeout value is set to 60 minutes. If a user performs various tasks in the OpenPages with Watson application for 45 minutes, then returns to view a report, they will be able to do so without having to log on to the reporting server again. However, if the reporting server has a smaller session inactivity value set, such as 15 minutes, then that same user would be required to log on to the reporting server. By default, the IBM WebSphere Application Server has a 30-minute timeout period. The default timeout period for IBM Cognos is 5400 seconds (equivalent to 90 minutes).

Setting session inactivity timeout values for application servers

You can set session inactivity timeout values for OpenPages application servers.

Before you begin

If you are using IBM OpenPages with Watson, you can also modify the value of the inactivity timeout period for the reporting server.

Set the timeout period for the IBM Cognos reporting server to a value greater than the application server timeout period. For more information, see [“Setting a session inactivity timeout value” on page 836](#).

Procedure

1. Prepare your environment.

IBM OpenPages with Watson

- a. Log on to the IBM OpenPages with Watson application server as a user with administrative permissions.
- b. Stop all OpenPages with Watson services. For more information, see [“Stopping application servers”](#) on page 843.

IBM OpenPages for IBM Cloud Pak for Data

Do the steps in [“Preparing the instance”](#) on page 46.

2. Go to the overrides directory.

IBM OpenPages with Watson

`<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/configDropins/overrides/`

Where `<server_name>` is the name of the application server.

IBM OpenPages for IBM Cloud Pak for Data

`/opt/ibm/wlp/usr/servers/defaultServer/configDropins/overrides`

3. In a text editor, open the `op-apps.xml` file and look for the following line:

```
<httpSession cookieSecure="true" invalidationTimeout="90m"/>
```

4. Set the `invalidationTimeout` parameter to the value in minutes. Save and close the file.
5. Do the following steps:

IBM OpenPages with Watson

- a. Restart all OpenPages with Watson services. For more information, see [“Starting application servers”](#) on page 841.
- b. If this is a load-balanced environment, repeat this procedure for each application server in the load-balanced environment.

IBM OpenPages for IBM Cloud Pak for Data

Do the steps in [“Backing up changes and implementing them across replicas”](#) on page 46.

What to do next

If you are using OpenPages with Watson, set the value of the inactivity timeout period for the reporting server.

Setting session inactivity timeout values for IBM Cognos

You can set a session inactivity timeout value for the IBM Cognos reporting server.

Procedure

1. Log on to the IBM Cognos server as a user with administrative permissions.
2. Go to the `<COGNOS_Home>/bin64` directory.

Table 259. Installation location of the IBM Cognos reporting server	
Operation system	Installation location
Windows	For example, <code><COGNOS_Home></code> is <code>C:\Program Files\ibm\cognos\analytics</code>
Linux	For example, <code><COGNOS_Home></code> is <code>/opt/ibm/cognos/analytics</code>

3. Double-click the `cogconfig.exe` file to start the IBM Cognos Configuration tool.
4. Expand **Security** and click **Authentication**.

5. Find the **Inactivity timeout in seconds** property and type a new value (in seconds) that is greater than the application server timeout value. For example, you could enter 7200 (equivalent to 120 minutes) if the application server timeout value is set to 90 minutes.
6. Save the configuration changes.
7. Restart the IBM Cognos server.

Setting the Cognos Application Firewall for browser security

To prevent URL redirection attacks in Cognos, enable Cognos Application Firewall and configure a host list in Cognos Configuration.

The backURL parameter is a standard (and optional) Cognos URL parameter. This parameter, shown in the following example, can be modified to redirect a user to any site. Therefore, the potential exists for an attacker to also use this parameter to redirect a user to a malicious site where sensitive information could be exposed, such as the user's cookie.

```
https://test.my-company.com/ibmcognos/cgi-bin/cognos.cgi?
b_action=xts.run&m=portal/launch.xts&ui.tool=CognosViewer&ui.action
=run&encoding=UTF8 &method=newQuery&backURL=http%3a%2f%2fwww.google.com
&m=qs%2fqs.xts&cafcontextid=&obj=%2fcontent%2fpackage%5b%40name%3d%270penPages%27%5d
```

The *IBM Cognos Analytics V11.1 Installation and Configuration Guide*, Configuration options chapter, section "Configure IBM Cognos Components to Use IBM Cognos Application Firewall", indicates that the standard method for performing positive validation of URL input parameters and data is to use the CAF (Cognos Application Firewall) setting in the Cognos Configuration tool. If the data does not match a CAF rule, it is rejected.

The IBM OpenPages with Watson Installer for OpenPages CommandCenter enables the Cognos Application Firewall (CAF) by default.

CAF can be configured with a list of host names, including port numbers and domains that a user can access through the backURL parameter. If a backURL parameter contains a host or a domain name that does not appear in the list, the request will be rejected. An error message, similar to the following, will be displayed to users who try to access invalid domains or hosts through the backURL parameter:

DPR-ERR-2079 Firewall Security Rejection. Your request was rejected by the security firewall.

The CAF setting has a known issue where enabling the firewall sometimes obscures useful error messages. For example, if a report author developed a report and that report had a logic flaw, a generic firewall error message (as shown previously) would be displayed rather than a more useful message containing information about the cause of the actual problem.

Although generic firewall messages are considered a safe way to protect information, this type of nondescript CAF error message would make troubleshooting of report authoring/development and certain kinds of configuration issues more difficult.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start IBM Cognos Configuration:
 - a) On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
 - b) Navigate to the <COGNOS_HOME>|bin64 or <COGNOS_HOME>|bin directory, where <COGNOS_HOME> is the installation location of the Cognos application.
 - c) Run the following command:

Windows:

```
cogconfig.bat
```


Linux:

```
./cogconfig.sh
```

3. In the **Explorer** window, under **Security**, click **IBM Cognos Application Firewall**.
4. In the **Properties** window, for the **Enable CAF validation** property, set the appropriate values.
By default, IBM Cognos Application Firewall is enabled.
5. Add host and domain names to the IBM Cognos list of valid names.
6. Save the configuration.

Browser security issues and running reports

Depending on how browser security is configured on client machines, Cognos reports might not launch successfully from the IBM OpenPages with Watson application user interface.

If a client machine that is using the Microsoft Edge browser is unable to run Cognos reports from the OpenPages with Watson application user interface, then do the following in **Control Panel > Internet Options**:

- Add each reporting server to the **Trusted sites** zone on that machine.
- On the **Trusted sites** page, clear the **Require server verification (https:) for all sites in this zone** checkbox.
- Modify the settings of the **Trusted Sites** zone and set the **Enable XSS Filter** property to **Disable**.
- Set the security level for the **Trusted sites** zone to **Low**.
- Click the **Custom level properties** for the **Trusted Sites** zone. Under **Downloads**, set **Automatic prompting for file downloads** and **File download** to **Enable**.
- Restart the browser

For information on adding trusted sites to the browser, use the browser documentation.

Browser locale settings and messaging issues

If a user sets the browser to an unsupported locale, logon and other IBM OpenPages with Watson application messages are displayed only in English.

To ensure proper display of messages in the browser, users must set their browsers to a supported locale. For a list of supported locales, see [Chapter 17, “Localizing text,” on page 559](#).

Browser errors about Content Security Policy

If you see errors in your browser about Content Security Policy and you use clustered application servers, do the following steps to resolve the issue.

Make a note of the server that is mentioned in the Content Security Policy error message.

Add the application server host and port number to the list of values in the **Platform > Security > Content-Security-Policy** setting. The setting uses the Content Security Policy tool syntax. For more information, see [Content Security Policy](#).

For more information, see [“Configure the HTTP response headers” on page 647](#).

Browser best practices

An IBM OpenPages with Watson browser session is active until one of three conditions is met.

- The user logs out of the OpenPages with Watson application.
- The session expires.
- The browser instance is closed.

The following are some suggested best practices for enhancing browser security that the users should be aware of:

- Logging off from OpenPages with Watson after they finish their work, and closing the browser window to ensure that no sensitive information is stored in the browser cache.
- Blocking their computers from external use when the users are not physically present - either by keeping their computers on stand-by or by locking their accounts.
- Copying (not clicking) a link to the OpenPages with Watson application from an e-mail and then pasting the link into the address bar of the browser window. After pasting the link, users should validate that the link they just pasted matches the link in the text of the e-mail message.
- Configuration of an inactivity timeout - administrators should set this to a desired security level that is based on commonly known levels of inactivity for their organization. For more information, see [“Setting a session inactivity timeout value”](#) on page 836.
- Configuration of the **Cross-site Scripting Filter** setting to check all HTTP GET requests sent to the OpenPages application server.

Chapter 24. Starting and stopping servers

You can start and stop the IBM OpenPages with Watson application servers, the database server, the Cognos server, and the search server.

Starting application servers

You can start IBM OpenPages with Watson in Windows and Linux environments.

In a Windows environment, you can start the OpenPages with Watson application servers by using Microsoft Windows services or by running a script.

In a Linux environment, you run a script to start the OpenPages with Watson application servers.

If you are running OpenPages in a load-balanced environment, you must start the server on the cluster administrator first before starting a cluster member.

Starting application servers by using Windows services

You can start IBM OpenPages with Watson application servers by using Microsoft Windows services.

About this task

The OpenPages application service is called `<server_name>Server<#>`, where `<server_name>` is the name of the application server. You can find the server name in the following locations:

- In the installation app on the application server card
- In the `deploy.properties` file in the `op_server_name` property.

In a load-balanced environment with vertical cluster members, each vertical cluster is numbered in sequence: `<server_name>Server1`, `<server_name>Server2`, and so on.

By default, the `<server_name>Server<#>` services are configured as `Manual` (the services do not start upon reboot). You can configure a service to start automatically. In Windows Services, change the service to `Automatic`.

For the IBM OpenPages with Watson application to run, all of the required Microsoft Windows services must be started and the services of supporting applications must be running.

Tip: Alternatively, you can start all application services by using a script. For more information, see [“Starting all application services by running a script \(Windows\)”](#) on page 842.

Procedure

1. Log on to the application server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Start each application service in sequence, starting with the `<server_name>Server1` service. Click the service, and then click **Start**.
The **Status** column might show **Running** before the startup process is done. Wait before starting the next application service.
Repeat this step for each application service that you want to start.
4. To set a service to start automatically after a restart, change its **Startup Type** to **Automatic**.
5. If you have horizontal application servers, repeat these steps on each of them.

Starting all application services by running a script (Windows)

The `StartAllServers.cmd` script, which is included with IBM OpenPages with Watson, starts all OpenPages application services on an application server.

Note: This information applies only to Microsoft Windows environments.

About this task

The script uses the following syntax:

```
StartAllServers.cmd [--clean]
```

The `--clean` option is not necessary for normal operation. IBM OpenPages Support might ask you to use this option when providing an interim fix, or if there is a suspected problem with the cached data. If you use this option, the server will be required to recompute any cached data at the next startup, which might take more time than a restart that reuses cached data.

Procedure

1. Log on to the OpenPages with Watson application server as a user with administrative privileges or as the OpenPages installation user, `opuser`.
2. Open a Command Prompt window (using the **Run as administrator** option) and do the following:
 - a) Navigate to the `<OP_HOME>\bin` directory.

Where `<OP_HOME>` is the installation location of the OpenPages with Watson application, for example: `c:\IBM\OpenPages`.

- b) Run the following command:

```
StartAllServers.cmd
```

The log file is: `<OP_HOME>\wlp-usr\servers\<server_name>\logs\messages.log`

3. If you have horizontal application servers, repeat these steps on each of them.

Starting all application servers by running a script (Linux)

The `startAllServers.sh` script, which is included with IBM OpenPages with Watson, starts all OpenPages application services on an application server.

Note: This information applies only to Linux environments.

About this task

The script uses the following syntax:

```
./startAllServers.sh [--clean]
```

The `--clean` option is not necessary for normal operation. IBM OpenPages Support might ask you to use this option when providing an interim fix, or if there is a suspected problem with the cached data. If you use this option, the server will be required to recompute any cached data at the next startup, which might take more time than a restart that reuses cached data.

The OpenPages application runs only if all of the services are started and all of the services for all supporting applications are running.

Procedure

1. Log on to the OpenPages application server as a user with administrative privileges or as the OpenPages installation user, `opuser`.
2. Open a shell window.

3. Go to the `<OP_HOME>/bin` directory.
4. Run the following script:

```
./startAllServers.sh
```

The application services on the application server are started.

The log file is: `<OP_HOME>/wlp-user/servers/<server_name>/logs/messages.log`

5. If you have horizontal application servers, repeat these steps on each of them.

Determining application readiness

This procedure lets you determine whether the application is ready to be accessed after starting up servers.

Procedure

1. Open the following log file:
`<OP_HOME>/wlp-user/servers/<server_name>/logs/messages.log`
Where `<server_name>` is the name of the application server.
2. Scroll to the end of the log file and search for the message `SRVE0242I: [op-apps] [/grc] [api-rest]: Initialization successful`. If this line appears, the server is running in production mode and the application is ready to be accessed.

Stopping application servers

You can stop IBM OpenPages with Watson application servers in Windows and Linux environments.

Stopping the application server prevents IBM OpenPages with Watson from being accessed.

Important: If you are running OpenPages with Watson in a load-balanced environment, stop `<server_name>Server1` last.

Stopping application servers by using Windows services

You can stop IBM OpenPages with Watson application servers by using Microsoft Windows services.

About this task

Stopping the application services prevents IBM OpenPages with Watson from being accessed.

Tip: Alternatively, you can stop all vertical cluster members on an application server by using a script. For more information, see [“Stopping all application servers in Windows by using a script” on page 843](#).

Procedure

1. Log on to the application server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Click the `<server_name>Server<#>` service and then click **Stop**. Repeat this step for each application service that you want to stop. If you have horizontal application servers, repeat these steps on each of them.

Stopping all application servers in Windows by using a script

The `StopAllServers.cmd` stops all OpenPages application services on an application server. The script stops the services in the proper sequence.

Stopping the application services prevents the OpenPages application from being accessed.

Procedure

1. Log on to the OpenPages with Watson application server as a user with administrative privileges.
2. Launch a Command Prompt window (using the **Run as administrator** option).
3. Navigate to the <OP_HOME>\bin directory.
4. Run the following command:

```
StopAllServers.cmd
```

5. If you have horizontal application servers, repeat these steps on each of them.

Stopping all application servers on Linux by using a script

The stopAllServers.sh script stops all OpenPages application services on an application server. The script stops the application services in the proper sequence.

Stopping the application services prevents the OpenPages application from being accessed.

Procedure

1. Log on to the OpenPages with Watson application server as a user with administrative privileges.
2. Open a shell window and navigate to the <OP_HOME>/bin directory.
3. Run the following command:

```
./stopAllServers.sh
```

The application services on the application server are stopped.

4. If you have horizontal application servers, repeat these steps on each of them.

Start or stop the global search services

You can start and stop the global search services by using operating system services or by using scripts.

Note: Do not combine the two methods. If you start global search as a Microsoft Windows service, for example, stop global search by stopping the Windows service.

Starting the global search services by using a script

You can start the global search services by running a script from a command line.

Before you begin

On the Windows operating system, disable the Microsoft Windows service that is called **IBM OpenPages GRC - Global Search**, if it is enabled. Otherwise, the StartSearchServers.cmd script interferes with the Windows services.

Make sure that the database server is reachable and is running. Otherwise, the search services will not connect and will not start.

Procedure

1. Start the search services:
 - For Windows, at a command prompt enter the following commands:

```
cd <SEARCH_HOME>\opsearchtools\  
StartSearchServers.cmd
```

- For Linux, at a command line, enter the following commands:

```
cd <SEARCH_HOME>/opsearchtools/  
./StartSearchServers.sh
```

2. Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform can be reached.
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.
If the verification fails, repeat the preceding step.
3. Log on to IBM OpenPages with Watson as an administrator.
4. Switch to the Standard UI.
5. Click **Administration > Global Search > Enable**.

Stopping the global search services by using a script

You can stop the global search services by running a script from a command line.

Before you begin

On the Windows operating system, disable the Microsoft Windows service that is called **IBM OpenPages GRC - Global Search**, if it is enabled. Otherwise, the `StopSearchServers.cmd` script interferes with the Windows services.

Procedure

1. Log on to IBM OpenPages with Watson as an administrator.
2. Switch to the Standard UI.
3. Click **Administration > Global Search > Disable**.
4. Stop the search services:
 - For Windows, at a command prompt, enter the following commands:

```
cd <SEARCH_HOME>\opsearchtools\  
StopSearchServers.cmd
```

- For Linux, at a command line, enter the following commands:

```
cd <SEARCH_HOME>/opsearchtools/  
./StopSearchServers.sh
```

5. For either Windows or Linux, verify that global search is fully stopped.
 - a) In the directory `<SEARCH_HOME>/opsearchtools/`, examine the files `opsearchtool_openpages.state` and `opsearchtool_folderacl.state` and verify that the PID value is -1.
 - b) Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform cannot be reached.
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.
If the stop verification fails, repeat the preceding step and then follow the steps in [“Forcing a reset of global search” on page 1103](#).

Starting the global search services on Windows

You can start global search as a Microsoft Windows service. The service is called **IBM OpenPages GRC - Global Search**.

About this task

By default, the service is set to start manually, but you can change the service to start automatically.

Note: Make sure that the database server is reachable and is up and running. Otherwise, the search services will not connect and will not start.

Procedure

1. Log on to the search server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Locate the service that is called **IBM OpenPages GRC - Global Search**.
4. Click **Start**.
5. If you want the service to start automatically when Windows starts, change the **Startup Type** to **Automatic**.
6. Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform can be reached.
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.
If the verification fails, repeat the preceding step.
7. Log on to IBM OpenPages with Watson as an administrator.
8. Switch to the Standard UI.
9. Click **Administration > Global Search > Enable**.

Starting the global search services on Linux

You can start global search as a service.

About this task

Use the steps in this topic as a guide. Depending on your environment and organization policies, you might decide to use a different method to set up the search service. If you want to use a different method, open the `openpages-search` file and check the commands, and the order of the commands. Modify the commands to meet the needs of your environment.

Note: Make sure that the database server is reachable and is up and running. Otherwise, the search services will not connect and will not start.

Procedure

1. Log on to the search server.
2. Open a shell as the root user.
3. Copy the `<SEARCH_HOME>/opsearchtools/openpages-search` file to the `/etc/init.d/` directory.
4. Copy the `<SEARCH_HOME>/opsearchtools/openpages-search-cfg` file to the `/etc/sysconfig/` directory.
5. Set the execution permission on the `openpages-search` file by running the following command:
`chmod +x /etc/init.d/openpages-search`
6. If you want the service to start automatically when the system restarts, run the following commands:

```
chkconfig --add openpages-search
chkconfig openpages-search on
service openpages-search start
```

7. Start the global search services by running the following command: `service openpages-search start`
8. Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform can be reached.
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.
If the verification fails, repeat the preceding step.

9. Log on to IBM OpenPages with Watson as an administrator.
10. Click **Administration > Global Search > Enable**.

Stopping the global search services

If global search is running as a service, you can use the operating system to stop the global search services.

About this task

If you used the `StartSearchServers.sh | .cmd` script to start the global search services, use the `StopSearchServers.sh | .cmd` script to stop the services. For more information, see [“Stopping the global search services by using a script”](#) on page 845.

Procedure

1. Log on to IBM OpenPages with Watson as an administrator.
2. Click **Administration > Global Search > Disable**.
3. Log on to the search server as a user with administrative privileges.
4. Stop the search services.

Windows:

- a) Click **Start > Windows Administrative Tools > Services**.
- b) Locate the service that is called **IBM OpenPages GRC - Global Search**.
- c) Click **Stop**.

On Linux, run the following command:

```
service openpages-search stop
```

5. Verify that global search is fully stopped.
 - a) In the directory `<SEARCH_HOME>/opsearchtools/`, examine the files `opsearchtool_openpages.state` and `opsearchtool_folderacl.state` and verify that the PID value is -1.
 - b) Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform cannot be reached.
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.
If the stop verification fails, repeat the preceding step and then follow the steps in [“Forcing a reset of global search”](#) on page 1103.

Start or stop the database services

You can start and stop the database services.

For more information, see the documentation that is provided with your database server:

IBM Db2

[Managing instances](#)

Oracle

[Starting Up and Shutting Down](#)

For examples, see [“Starting and stopping the Oracle database server in a Windows environment”](#) on page 848 or [“Starting and stopping the Oracle database server in Linux environments”](#) on page 848.

Starting and stopping the Oracle database server in a Windows environment

The following steps show an example of how to start or stop an Oracle database server by using Windows services.

About this task

For more information, see the Oracle [documentation](#).

Table 260. Oracle services for OpenPages on Windows	
Service Name	Description
Oracle<ORACLE_HOME>TNSListener	Runs the Oracle Database listener service that connects the user to the Oracle database instance.
OracleService<SID>	Used to start and stop the Oracle database instance. Where <SID> represents the database instance identifier, for example OP.
OracleVssWriter<SID>	Where <SID> represents the database instance identifier, for example OP.

Procedure

1. Log on to the database server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. For each database service listed in [Table 260 on page 848](#), do the following:
 - To start the server, right-click the service name and select **Start**.
 - To stop the server, right-click the service name and select **Stop**.

Starting and stopping the Oracle database server in Linux environments

The following steps show an example of how to start or stop an Oracle database.

For more information, see the Oracle [documentation](#).

Procedure

1. Log on to the database server as a user with administrative privileges.
2. In a shell window, navigate to the following directory:

```
<ORACLE_HOME>/bin
```

For example: /opt/oracle/app/product/19.0/dbhome_1/bin.

3. To start Oracle, do the following steps.

- a) Log in to SQL*Plus.

```
sqlplus / as sysdba
```

- b) Run the following command to start Oracle.

```
startup
```

4. To stop Oracle, do the following steps.

- a) Log in to SQL*Plus.

```
sqlplus / as sysdba
```

b) Run the following command to stop Oracle.

```
stop immediate
```

Starting and stopping the Cognos services

There are different procedures to start or stop the Cognos services in the Windows and Linux environments. The services are the IBM Cognos service and the OpenPages Framework Model Generator service

These procedures are:

- [“Using the IBM Cognos configuration tool to start and stop the IBM Cognos service” on page 849](#)
- [“Using the Windows operating system to start and stop the IBM Cognos service” on page 849](#)
- [“Using the Linux operating system to start and stop the IBM Cognos service” on page 850](#)
- [“Starting and stopping the OpenPages with Watson Framework Model Generator service on Windows” on page 850](#)
- [“Starting and stopping the OpenPages with Watson Framework Model Generator service on Linux” on page 850](#)

Using the IBM Cognos configuration tool to start and stop the IBM Cognos service

You can use the IBM Cognos Configuration tool to start or stop the IBM Cognos service.

The IBM Cognos Configuration tool displays the status of the start-up, which can be helpful with troubleshooting.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start the IBM Cognos Configuration tool as follows:
 - a) Open a command prompt (using the **Run as administrator** option), or a Linux shell, and navigate to the `<COGNOS_HOME>/bin` directory.
`<COGNOS_HOME>` represents the installation location of the Cognos application.
 - b) Run one of the following commands to open the tool:
Windows
`cogconfig.bat`
Linux
`./cogconfig.sh`
3. Do one of the following:
 - To start the server, click **Actions > Start**. It might take several minutes for the service to start the first time.
If the **Start** option is not available, the service has already started.
 - To stop the service, click **Actions > Stop**.

Using the Windows operating system to start and stop the IBM Cognos service

Use the following steps to start or stop the IBM Cognos service in a Windows environment using Windows Services.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Do one of the following:
 - To start the server, right-click the IBM Cognos service and select **Start**.
 - To stop the server, right-click the IBM Cognos service and select **Stop**.

Using the Linux operating system to start and stop the IBM Cognos service

Use the following steps to start or stop the IBM Cognos service in a Linux environment using command-line scripts.

Procedure

1. Log on to the reporting server as a non-root user with administrative privileges.
2. Open a shell window and navigate to the `<COGNOS_HOME>/bin64` directory
Where `<COGNOS_HOME>` is the installation location of the Cognos application.
3. Do one of the following:
 - To start the service, enter the following command: `./cogconfig.sh -s`
 - To stop the service, enter the following command: `./cogconfig.sh -stop`

Starting and stopping the OpenPages with Watson Framework Model Generator service on Windows

Use the following steps to start or stop the IBM OpenPages with Watson Framework Model Generator service in a Microsoft Windows environment.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Do one of the following:
 - To start the server, right-click the IBMOpenPagesFrameworkModelGenerator service and select **Start**.
 - To stop the server, right-click the IBMOpenPagesFrameworkModelGenerator service and select **Stop**.

Starting and stopping the OpenPages with Watson Framework Model Generator service on Linux

Use the following steps to start or stop the IBMOpenPagesFrameworkModelGenerator service in a Linux environment.

Procedure

1. Log on to the reporting server as a non-root user with administrative privileges.
2. Open a shell window as a user with administrative privileges and navigate to the following directory:

```
<CommandCenter_Home>/wlp/bin
```

Where `<CommandCenter_Home>` is the installation location of IBM OpenPages CommandCenter. By default, this is: `/opt/IBM/OpenPages/CommandCenter`.

3. To start the service, run the following command.

```
./server start IBMOpenPagesFrameworkModelGenerator
```

4. To stop the service, run the following command.

```
./server stop IBMOpenPagesFrameworkModelGenerator
```


Chapter 25. Comparing IBM OpenPages with Watson environments

You can find differences between two environment configuration XML files by using **Compare Environments**. Use Compare Environments to identify and resolve issues before you migrate configurations from one environment to another.

Note: This feature is not applicable in IBM OpenPages for IBM Cloud Pak for Data.

Compare Environments compares XML files that you generate in each environment. You can generate the XML files by using Export Configuration or by using ObjectManager. Compare Environments looks at the XML files and identifies any differences in the files. Compare Environments also uses validation rules to check the XML files for any errors and for changes that might cause issues during a migration.

Compare Environments

Select Object Manager files to compare:

Source File:

source-env-profiles-mig-072717125528-op-config.xml

Browse...

Target File:

target-env-profiles-mig-072717011344-op-config.xml

Browse...

* Categories

☐ Application Text

☐ Field Groups

☒ Object Profiles

☐ Object Text

☐ Object Type Associations

☐ Object Types

☐ Settings

* Severity

☒ Error

☒ Warning

☒ Info

* Change Type

☒ In Source, Not in Target

☒ In Target, Not in Source

☒ Validation Issue

Compare

Result Summary

2

Differences

0

Errors

0

Warnings

Export Details

Figure 61. Comparing profiles in a source and target environment

	A	B	C	D	E	F	G	H
	Top Category	Severity	Change Type	Context	XML Element	Description	Source XML Line No.	Target XML Line No.
1	ObjectProfiles	INFO	NOTPRESENT	NewVendor	objectProfile	objectProfile NewVendor is present in target but not present in source		135182
2	ObjectProfiles	INFO	NOTPRESENT	NewVendor	objectProfileViews	objectProfileViews NewVendor is present in target but not present in source		336224
3								
4								
5								
6								
7								

Figure 62. Results of the comparison: A profile does not exist in the source environment

The source and target files can be from environments that are running different versions of IBM OpenPages with Watson. Further, you can run Compare Environments on a system that is running a version that is different from both the source and target environments.

Note: Compare Environments compares only the content of the XML files that you specify. It does not compare any other aspects of your source and target environments.

Compare Environments can use significant system resources. Follow these guidelines when you are using it:

- Do not run Compare Environments on production environments.
- Do not run Compare Environments on servers that are busy with other activities.
- The XML files that you want to compare might be very large. If so, the time it takes to upload the files to the system might take several minutes or longer. Consider this factor before using a connection with slow upload speeds.

Use the following process to compare environments:

- Decide what you want to compare.
- Generate an XML file in the source environment.
- Generate an XML file in the target environment.
- Use the filters on the **Compare Environments** page to filter on the configuration data that you want to compare.

By using the filters, you can reduce the amount of time it takes to compare the XML files. Filters can also help you to focus on the results that you need by removing potentially distracting information from the results. Comparison results can include hundreds of thousands of rows.

- Run the comparison.
- Download the detailed results.
- Analyze the results.
- Fix any errors and review any warning messages.

When you compare environments, keep the following points in mind:

- Compare Environments uses the source environment file as the point of reference. If you reverse the source and target files, the results are different, and this is expected.
- Compare Environments ignores any data that it does not support.
- The source environment, the target environment, and the environment where you run Compare Environments can each have a different version of OpenPages installed.
- Currency fields are different from other fields. Currency fields have a different XML structure from other types of fields.

- Currency fields are represented in the XML like a field group (by using the `bundleType` element).
- Currency fields are implemented with a nested field group that contains the currency attributes, such as the exchange rate, base amount, local amount, currency code, base code, and so on. If Compare Environments finds differences in a currency field, it logs the change at both the currency field level and at the nested field group level.
- When Compare Environments finds an element that is missing from the source file or from the target file, it logs the difference at the level of that element only. Compare Environments does not log differences for the element's children.

The only exception to this rule is for currency fields. If a currency field is missing, Compare Environments logs the missing field and its child field group.

- The line numbers that you see in the output might be different from what you expect to see based on the XML file. The line numbers that are shown in the output are the line numbers where the closing tags occur in the XML file. An element can span several lines, for example if the element has attributes on different lines.

For example, the line number reported in the output for the following `Year` field is 83, the line on which the closing tag occurs.

```
81     <includedField name="Year"
82         readOnly="false"
83         required="false">
```

- If you added a custom object type in OpenPages, the object type definition in the XML file contains at least two `contentTypeRelationship` elements, attachment and association. These content type relationships are added by default. Compare Environments reports on these elements.

For example, suppose that you added a custom object type in the source environment and it does not exist in the target environment. When you defined the custom object type, you set up a parent association. When you generate and compare the XML files, Compare Environments logs two information messages about object type associations: one about the parent object association that you added, and another about the attachment association, which was added by default.

- In certain cases, when you use the **Administration** pages, default configuration elements are created in the background. These changes might not be apparent in the user interface at the time.

For example, when you view the details of a profile for the first time and add an included object type such as `SOXBusEntity`, default entries for the Overview navigation view are added automatically. If you export object profiles without making any additional changes, the XML file includes the additional elements for the Overview view in the object profile.

This video demonstrates how to use Compare Environments to identify and resolve issues before you migrate configurations from one environment to another (Standard UI):

https://youtu.be/P_0zYBtZE0k

Review configuration settings

Before you compare environments, review the configuration settings that impact the process to ensure that they meet your requirements.

Settings > Applications > Common > Max File Upload Size

This setting specifies the maximum size of an upload. The limit is on the total upload size of both files. If your XML files are large, you might need to increase the value of this setting. Also, consider using the filters on the **Export Configuration** page to reduce the file size. Or, if you are using ObjectManager, change the ObjectManager properties to generate smaller files.

After you change this setting, restart the application server. For more information, see [“Configuring large files for upload”](#) on page 617.

Settings > Platform > CompareEnvironments > Export Max Rows

This setting specifies the maximum number of rows that are exported in the detailed results spreadsheet. If you are working with large files, you might need to increase the value of this setting. If

you do so, you might also need to increase the value of the Max Memory setting. For more information, see [“Maximum number of rows to export from the Compare Environments tool” on page 638](#).

Settings > Platform > CompareEnvironments > Max Memory

This setting specifies the maximum Java heap size that can be used by Compare Environments. For more information, see [“Java heap size for the Compare Environments tool” on page 638](#).

Supported items

Compare Environments supports the comparison of many configuration items. Compare Environments ignores any items that it does not support.

Compare Environments supports the following items:

- Object types, including object type associations (parent or child), associated field groups, and file type information
- Field groups
- Fields, including field types, display types, and display type attributes
- Computed field details, including equation, primary namespace, alternative namespaces, object ID, and reporting period ID
- Enumerated string values for enumerated string fields
- Object profiles, including object profile views
- Settings
- Object text
- Application text

For information about how items are represented in XML, export results from the Compare Environments tool and then click the **Legend** tab of the exported workbook.

Compare Environments does not support some items, for example:

- Filters
- Field dependencies
- Dependent picklists
- Security (groups, users, role templates, custom security, security rules)
- Object resets
- Configuration settings for apps and features that have their own configuration pages, such as the approval app, IBM OpenPages Loss Event Entry, IBM OpenPages Regulatory Compliance Management, and classifiers for cognitive services
- Questionnaire Assessments
- Triggers
- Custom query subjects
- JSPs
- For activity views, a maximum of three levels of associated object types is supported
- Instance data

Prepare the files to compare

To compare two environments, you need to export an XML file from each environment.

You can use Export Configuration or ObjectManager to export files from the source and target environments.

Export Configuration XML files might include other types of items in addition to the ones you selected for export. For example, if you export a profile, Export Configuration also exports items that the profile depends on, such as views.

Use the same method to generate the XML file for each environment whenever possible. If you use a different method for each file, the results include a larger number of differences than if you had used the same method for the two files. These additional differences are expected, since the XML files generated by Export Configuration and by ObjectManager can contain different levels of detail.

Preparing files by using Export Configuration

You can prepare the XML files to compare by using Export Configuration.

Procedure

1. Export configurations in the source environment.

For more information, see [“Exporting configuration items from the source environment \(Standard UI\)” on page 874](#).

The tool generates a .jar file.

2. Download the .jar file.
3. Decompress the .jar file.

Note: You might need to change the extension to .zip, depending on the data extraction tool that you are using.

4. Go to the loader-data directory and locate the openpages-env-mig-<timestamp id>-op-config.xml file.

5. Give the file a meaningful name.

For example, source-openpages-env-mig-<timestamp id>-op-config.xml

6. Repeat these steps in the target environment. Give the XML file a meaningful name such as target-openpages-env-mig-<timestamp id>-op-config.xml.

Preparing files by using ObjectManager

You can prepare the XML files to compare by using ObjectManager.

Procedure

1. In the source environment, go to the <OP_HOME>/bin/ directory.

2. Edit the <OP_HOME>/bin/ObjectManager.properties file. Configure the areas that you want to export.

- To export all configuration data, set the following setting to true:

```
configuration.manager.migrate.configuration.objects=true
```

This setting extracts more data than is supported by the Compare Environments tool. The Compare Environments tool ignores any data that is not supported.

- To export all configuration data that **Compare Environments** supports, see [“ObjectManager properties for comparing environments” on page 858](#).
- To specify the configuration data that you want to export, look for the settings that begin with configuration.manager.dump.*

The ObjectManager.properties file contains over 45 settings of this type. For more information, see [“Settings in the ObjectManager.properties file ” on page 893](#).

To export data, change the value of a setting to true. For example, to export all fields and field groups, use the following setting:

```
configuration.manager.dump.bundle.type=true
```

For more information, see [“Modifying the ObjectManager properties file”](#) on page 892.

3. Save the ObjectManager.properties file.
4. Run the following command:

```
ObjectManager.sh d c <OP admin user> <OP admin user password>  
    <output directory> <output file prefix>
```

The XML output file is created in the output directory that you specified and is named *<output file prefix>-op-config.xml*.

5. Repeat these steps in the target environment.

ObjectManager properties for comparing environments

If you want to export all of the configurations that Compare Environments supports, use the following settings in the *<OP_HOME>/bin/ObjectManager.properties* file.

```
configuration.manager.dump.modules=false  
configuration.manager.dump.file.types=false  
configuration.manager.dump.bundle.types=true  
configuration.manager.dump.file.upload.content.types=true  
configuration.manager.dump.jsp.based.content.types=true  
configuration.manager.dump.content.type.relationship.sets=true  
configuration.manager.dump.app.permissions=false  
configuration.manager.dump.actors=false  
configuration.manager.dump.actor.group.memberships=false  
configuration.manager.dump.actor.object.profile.associations=false  
configuration.manager.dump.admin.objectprofile.views=true  
configuration.manager.dump.non.form.based.resources=false  
configuration.manager.dump.form.based.content.types=true  
configuration.manager.dump.form.based.resources=false  
configuration.manager.dump.channels=false  
configuration.manager.dump.resource.sets=false  
configuration.manager.dump.associated.resources=false  
configuration.manager.dump.rule.sets=false  
configuration.manager.dump.rule.set.execute.sessions=false  
configuration.manager.dump.registry=true  
configuration.manager.dump.object.profiles=true  
configuration.manager.dump.recursive.hierarchy=false  
configuration.manager.dump.date.dimension.type=false  
configuration.manager.dump.object.type.dimension=false  
configuration.manager.dump.date.dimension.type.associations=false  
configuration.manager.dump.locales=false  
configuration.manager.dump.application.string.key.categories=true  
configuration.manager.dump.application.string.keys=true  
configuration.manager.dump.application.strings=true  
configuration.manager.dump.recursive.hierarchy.strings=false  
configuration.manager.dump.date.dimension.type.strings=false  
configuration.manager.dump.object.type.dimension.strings=false  
configuration.manager.dump.error.strings=false  
configuration.manager.dump.object.strings=true  
configuration.manager.dump.job.types=false  
configuration.manager.dump.currency.exchange.rates=false  
configuration.manager.dump.currencies=false  
configuration.manager.dump.query.definitions=false  
configuration.manager.dump.user.preferences=false  
configuration.manager.dump.role.templates=false  
configuration.manager.dump.role.administrators=false  
configuration.manager.dump.role.assignments=false  
configuration.manager.dump.field.dependency=false  
configuration.manager.dump.field.dependency.picklist=false  
configuration.manager.dump.subsystem.exclusion.fields=false
```

Comparing environments

You can compare environments to find differences between two environment configuration XML files.

Before you begin

You must have the **Compare Environments** application permission to see the **Compare Environments** menu item. The location of the permission in a role template is **All Permissions > SOX > Administration > Compare Environments**.

Prepare the XML files that you want to compare. For more information, see [“Prepare the files to compare” on page 856](#).

Procedure

1. Log in as a user with the **Compare Environments** permission.
2. Click **Administration > Compare Environments**.
3. Select the XML file for the source environment.
4. Select the XML file for the target environment.
5. Choose the categories that you want to include.
6. Choose the severity levels that you want to include.
7. Select the types of changes you want to include:
 - **In Source, Not in Target:** Find items that exist in the source environment XML file and do not exist in the target.
 - **In Target, Not in Source:** Find items that exist in the target environment XML file and do not exist in the source.
 - **Validation Issue:** Find validation issues.
8. Click **Compare**.

Depending on the size of the XML files, the options that you selected, and your upload connection speed, the process might take several minutes to complete.

Important: Stay on the **Compare Environments** page until the process completes. If you leave the page, you will need to select the files again and re-run the comparison to get the results.
9. Click **Export Details**. Save or open the .xlsx file.
10. Analyze the results. For more information, see [“Interpret results” on page 859](#).

Interpret results

When you export results from Compare Environments, you get a .xlsx file. The workbook provides details about the comparison, along with the results.

Context tab

Lists the options that you used to do the comparison.

Differences tab

Lists the differences that were found. Look for any errors or warnings.

Table 261. Descriptions of the columns on the Differences tab	
Column	Description
Top Category	The overall category of the difference, error, or warning that was found.

Table 261. Descriptions of the columns on the Differences tab (continued)	
Column	Description
Severity	The severity of the issue. INFO: An information message only. No action is required. ERROR: An issue that must be fixed before you can use the XML files to migrate from the source to the target. WARNING: An issue that might impact migration. Investigate and make any changes that are needed.
Change Type	The type of issue that was found. ADD: An item exists in the source XML file but does not exist in the target XML file. When you migrate, the item will be added to the target environment. NOT PRESENT: An item exists in the target XML file but does not exist in the source XML file. UPDATE: An item exists in both the source and target, but a difference was found. When you migrate, the target environment will be updated with the value from the source XML file. REMOVE: An item exists in the target XML file but does not exist in the source XML file. When you migrate, the item will be removed from the target environment. CONFLICT: A validation issue was found in either the source or target XML file.
Context	The path to the XML element where the error, warning, or difference was found.
XML Element	The XML element that contains the error, warning, or difference.
Description	A description of the error, warning, or difference. You can find more information about errors and warnings on the Validation_Rules tab.
Source XML Line No.	The line number in the source XML file. If an element spans multiple lines, the tool reports the line number where the closing tag is located.
Target XML Line No.	The line number in the target XML file. If an element spans multiple lines, the tool reports the line number where the closing tag is located.
Attribute Changed	The name of the attribute that was changed.
Source Value	The value in the source XML file.
Target Value	The value in the target XML file.

Table 261. Descriptions of the columns on the Differences tab (continued)	
Column	Description
Context <i>n</i>	Details about where the error, warning, or difference was found. These columns parse the path in the Context column into individual elements. Each column contains an XML element and its value. For example, if an issue was found in a field, the Context 1 column displays <code>bundleType: field_group_name</code> and the Context 2 column displays <code>propertyType: field_name</code>.

Validation_Rules tab

Lists the rules that the tool uses to validate the source and target XML files.

Legend tab

Lists the configuration items that the tool compares and the name of the elements that represent them in the XML files.

If you want to migrate from the source environment to the target environment, fix any errors and review all warnings. Regenerate the XML files, and then run the Compare Environments tool again. Verify the results.

Errors, warnings, and how to fix them

When you run compare environments with the **Validation Issues** option selected, Compare Environments uses validation rules to check the XML files. If issues are found, it logs errors and warnings.

In many cases, an error or warning can be fixed in various ways. Analyze each error and warning to determine how to address it.

In some cases, you can resolve an issue by making a change in the source environment and then exporting a new XML file.

In other cases, the error or warning cannot be resolved by modifying the source environment. Instead, you can modify the source XML file to fix the error or warning manually.

- Edit the source XML file in a text editor to fix the error or warning.
- Run Compare Environments with the updated XML file to verify that the error or warning is fixed.

Important: The solutions that are described on the Validation_Rules tab for each error and warning are suggestions only.

Example: A field group exists in the source environment, but not in the target

Suppose that the source environment has a field group that is called CustomFG. The field group does not exist in the target environment.

You export field groups from each environment by using **Export Configuration**. You then compare the two XML files by using **Compare Environments**. You choose to compare all categories. You also choose to include errors, warnings, and information messages in the results.

In this case, the tool generates the following message:

	A	B	C	D	E	F
	Top Category	Severity	Change Type	Context	XML Element	Description
1	FieldGroups	INFO	ADD	CustomFG	bundleType	bundleType ID_CustomFG is not present and will be added
2						
3						
4						
5						
6						
7						

Figure 63. Results of the export: A field group is not in the target environment

The bundleType message indicates that the field group that is called CustomFG is not in the target environment.

If you added fields to the CustomFG field group, you also see messages about the fields. For example, if the CustomFG field group has a field that is called CustomField and this field does not exist in the target, you see the following messages:

	A	B	C	D	E	F
	Top Category	Severity	Change Type	Context	XML Element	Description
1	FieldGroups	INFO	ADD	CustomFG	bundleType	bundleType ID_CustomFG is not present and will be added
2	FieldGroups	INFO	ADD	CustomFG > CustomField	propertyType	propertyType ID_CustomFG:ID_Field is not present
3	ObjectText	INFO	ADD	French > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
4	ObjectText	INFO	ADD	German > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
5	ObjectText	INFO	ADD	Italian > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
6	ObjectText	INFO	ADD	Japanese > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
7	ObjectText	INFO	ADD	Portuguese > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
8	ObjectText	INFO	ADD	Report Design Language > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
9	ObjectText	INFO	ADD	Simplified Chinese > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
10	ObjectText	INFO	ADD	Spanish > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
11	ObjectText	INFO	ADD	Traditional Chinese > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
12	ObjectText	INFO	ADD	U.K. English > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
13	ObjectText	INFO	ADD	U.S. English > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
14						

Figure 64. Results of the export: A field group and its fields are not in the target environment

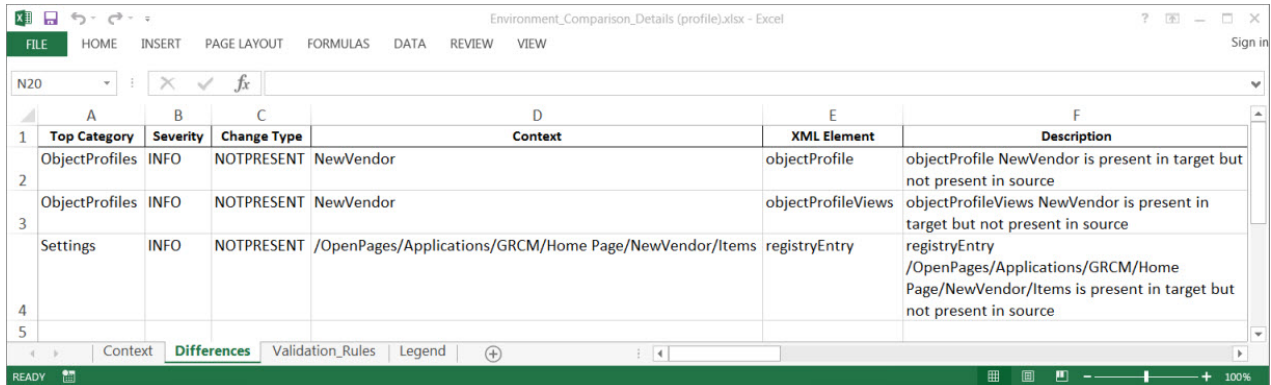
- The bundleType message indicates that the CustomFG field group is not in the target environment.
- The propertyType message indicates that the field that is called CustomField is not in the target environment.
- The fieldString messages are generated for each locale that is defined for the field called CustomField.

Example: A profile exists in the target environment, but not in the source

Suppose that the target environment has a profile that is called NewVendor that is based on the VRM Vendor profile. The NewVendor profile does not exist in the source environment.

You export object profiles from each environment by using **Export Configuration**. You then compare the two XML files by using **Compare Environments**. You choose to compare all categories. You also choose to include errors, warnings, and information messages in the results.

In this case, the tool generates the following messages:



	A	B	C	D	E	F
	Top Category	Severity	Change Type	Context	XML Element	Description
1	ObjectProfiles	INFO	NOTPRESENT	NewVendor	objectProfile	objectProfile NewVendor is present in target but not present in source
2	ObjectProfiles	INFO	NOTPRESENT	NewVendor	objectProfileViews	objectProfileViews NewVendor is present in target but not present in source
3	Settings	INFO	NOTPRESENT	/OpenPages/Applications/GRCM/Home Page/NewVendor/Items	registryEntry	registryEntry /OpenPages/Applications/GRCM/Home Page/NewVendor/Items is present in target but not present in source
4						
5						

Figure 65. Results of the export: A profile does not exist in the source environment

- The objectProfile message indicates that the profile that is called NewVendor does not exist in the source environment.
- When the NewVendor profile was created, a new view definition was created automatically. The objectProfileViews message indicates that this view definition does not exist in the source environment.
- When the NewVendor profile was created, a new registry setting was added automatically. The registryEntry message indicates that this setting does not exist in the source environment.

If the profile uses fields groups, fields, or other items that are not in the source environment, you see messages about these differences also.

Example: A custom object type exists in the target environment, but not in the source

Suppose that the target environment has a custom object type that is not in the source environment.

The custom object has the following characteristics:

- Name: CustomObject2
- Parent: Incident
- Included field groups: OPSS-Inc-IT

You export object types from each environment by using **Export Configuration**. You then compare the two XML files by using **Compare Environments**. You choose to compare all categories. You also choose to include errors, warnings, and information messages in the results.

In this case, the tool generates the following messages:

	A	B	C	D	E	F
	Top Category	Severity	Change Type	Context	XML Element	Description
1	ObjectText	INFO	NOTPRESENT	French > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
2	ObjectText	INFO	NOTPRESENT	German > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
3	ObjectText	INFO	NOTPRESENT	Italian > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
4	ObjectText	INFO	NOTPRESENT	Japanese > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
5	ObjectText	INFO	NOTPRESENT	Portuguese > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
6	ObjectText	INFO	NOTPRESENT	Report Design Language > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
7	ObjectText	INFO	NOTPRESENT	Simplified Chinese > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
8	ObjectText	INFO	NOTPRESENT	Spanish > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
9	ObjectText	INFO	NOTPRESENT	Traditional Chinese > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
10	ObjectText	INFO	NOTPRESENT	U.K. English > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
11	ObjectText	INFO	NOTPRESENT	U.S. English > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
12	ObjectTypeAssociations	INFO	NOTPRESENT	parent=Incident;child=CustomObject2;type=Association;	contentTypeRelationship	contentTypeRelationship parent=Incident;child=CustomObject2;type=Association; is present in target but not present in source
13	ObjectTypeAssociations	INFO	NOTPRESENT	parent=Incident;child=CustomObject2;type=Attachment;	contentTypeRelationship	contentTypeRelationship parent=Incident;child=CustomObject2;type=Attachment; is present in target but not present in source
14	ObjectTypes	INFO	NOTPRESENT	CustomObject2	contentType	contentType CustomObject2 is present in target but not present in source
15						
16						

Figure 66. Results of the export: A custom object does not exist in the source environment

- The contentType message indicates that the object type that is called CustomObject2 does not exist in the source environment.
- When you created the CustomObject2 object type, you defined a parent relationship with the Incident object type. The contentTypeRelationship message in row 13 indicates that the parent association is not in the source environment.
- Although you did not define an attachment association when you created the CustomObject2 object type, the association was added by default when you created it. The contentTypeRelationship message in row 14 indicates that the association is not in the source environment.
- The objectTypeString messages are generated for each locale.

Log files for the Compare Environments tool

Each time that you run the Compare Environments tool, a log file is created.

The log files are located in the `<OP_HOME>/aurora/logs` directory.

The naming convention for the log files is `<openpages server instance name><unique session id>-<start java timestamp>-compareenvironments.log`.

Example:

```
opapp-OPNode1Server11982-1499351409947-compareenvironments.log
```

Delete old Compare Environments log files periodically to clean up the `<OP_HOME>/aurora/logs` directory.

The log files for the Compare Environments tool are included when you run the LogCollector tool. For more information, see [“Collect log files and diagnostic data” on page 826](#).

Chapter 26. Migrating OpenPages environments

If your organization has multiple OpenPages environments, you can migrate both the configuration information and the metadata from one environment to another. Migration means exporting from a source environment and importing into a target environment.

You can use the **Export Configuration** tool to create a migration file, which can then be imported by using the **Import Configuration** tool. You can also use **Import Configuration** to import files in XML format. For more information, see [“Supported migration items” on page 866](#).

Tip: You can also use ObjectManager, a command line interface (CLI) tool, to migrate configuration changes. For more information, see [Chapter 27, “The ObjectManager tool,” on page 881](#).

An OpenPages environment is a set of OpenPages servers that target a single database instance, inclusive of that database instance. For example, your organization might have Development, UAT, and Production environments.

The environment from which you want to export data is referred to as the *source* and the environment into which you want to import data is referred to as the *target*.

The source and target environments must have the same version and patch level of OpenPages.

Settings that apply to environment migration

The environment migration settings are found in the **Applications > GRCM > Environment Migration** folder hierarchy.

For instructions on accessing the settings page, see [Chapter 19, “Viewing the Configuration and Settings page,” on page 597](#).

Tip: To author an XML settings path, add the OpenPages folder at the beginning of the path. For example: /OpenPages/Applications/GRCM/Environment Migration/

The following settings apply to both the Task Focused UI and the Standard UI.

Table 262. Environment migration settings	
Setting	Definition
Export File Name Prefix	Prefix to be added to the environment migration export file name. The default prefix, openpages, is used if no value is given. Prefix length is limited to 15 characters. If the prefix is longer than 15 characters, it is truncated. Important: - The following characters cannot be used in the prefix: <code>\ / * : { } [] " ?</code> - Do not use the special characters as defined in CJK Compatibility Ideographs Unicode Block Name and the four-byte characters as defined in the CJK Unified Ideographs EXTENSION-B Unicode Block Name in the prefix. The special characters to avoid are: 𠂇, 𠂈, 𠂉, 𠂊, 𠂋, 𠂌, 𠂍, 𠂎, 𠂏, 𠂐, 𠂑, 𠂒, 𠂓, 𠂔, 𠂕, 𠂖, 𠂗, 𠂘, 𠂙, 𠂚, 𠂛, 𠂜, 𠂝, 𠂞, 𠂟, 𠂠, 𠂡, 𠂢, 𠂣, 𠂤, 𠂥, 𠂦, 𠂧, 𠂨, 𠂩, 𠂪, 𠂫, 𠂬, 𠂭, 𠂮, 𠂯, 𠂰, 𠂱, 𠂲, 𠂳, 𠂴, 𠂵, 𠂶, 𠂷, 𠂸, 𠂹, 𠂺, 𠂻, 𠂼, 𠂽, 𠂾, 𠂿, 𠃀, 𠃁, 𠃂, 𠃃, 𠃄, 𠃅, 𠃆, 𠃇, 𠃈, 𠃉, 𠃊, 𠃋, 𠃌, 𠃍, 𠃎, 𠃏, 𠃐, 𠃑, 𠃒, 𠃓, 𠃔, 𠃕, 𠃖, 𠃗, 𠃘, 𠃙, 𠃚, 𠃛, 𠃜, 𠃝, 𠃞, 𠃟, 𠃠, 𠃡, 𠃢, 𠃣, 𠃤, 𠃥, 𠃦, 𠃧, 𠃨, 𠃩, 𠃪, 𠃫, 𠃬, 𠃭, 𠃮, 𠃯, 𠃰, 𠃱, 𠃲, 𠃳, 𠃴, 𠃵, 𠃶, 𠃷, 𠃸, 𠃹, 𠃺, 𠃻, 𠃼, 𠃽, 𠃾, 𠃿, 𠄀, 𠄁, 𠄂, 𠄃, 𠄄, 𠄅, 𠄆, 𠄇, 𠄈, 𠄉, 𠄊, 𠄋, 𠄌, 𠄍, 𠄎, 𠄏, 𠄐, 𠄑, 𠄒, 𠄓, 𠄔, 𠄕, 𠄖, 𠄗, 𠄘, 𠄙, 𠄚, 𠄛, 𠄜, 𠄝, 𠄞, 𠄟, 𠄠, 𠄡, 𠄢, 𠄣, 𠄤, 𠄥, 𠄦, 𠄧, 𠄨, 𠄩, 𠄪, 𠄫, 𠄬, 𠄭, 𠄮, 𠄯, 𠄰, 𠄱, 𠄲, 𠄳, 𠄴, 𠄵, 𠄶, 𠄷, 𠄸, 𠄹, 𠄺, 𠄻, 𠄼, 𠄽, 𠄾, 𠄿, 𠅀, 𠅁, 𠅂, 𠅃, 𠅄, 𠅅, 𠅆, 𠅇, 𠅈, 𠅉, 𠅊, 𠅋, 𠅌, 𠅍, 𠅎, 𠅏, 𠅐, 𠅑, 𠅒, 𠅓, 𠅔, 𠅕, 𠅖, 𠅗, 𠅘, 𠅙, 𠅚, 𠅛, 𠅜, 𠅝, 𠅞, 𠅟, 𠅠, 𠅡, 𠅢, 𠅣, 𠅤, 𠅥, 𠅦, 𠅧, 𠅨, 𠅩, 𠅪, 𠅫, 𠅬, 𠅭, 𠅮, 𠅯, 𠅰, 𠅱, 𠅲, 𠅳, 𠅴, 𠅵, 𠅶, 𠅷, 𠅸, 𠅹, 𠅺, 𠅻, 𠅼, 𠅽, 𠅾, 𠅿, 𠆀, 𠆁, 𠆂, 𠆃, 𠆄, 𠆅, 𠆆, 𠆇, 𠆈, 𠆉, 𠆊, 𠆋, 𠆌, 𠆍, 𠆎, 𠆏, 𠆐, 𠆑, 𠆒, 𠆓, 𠆔, 𠆕, 𠆖, 𠆗, 𠆘, 𠆙, 𠆚, 𠆛, 𠆜, 𠆝, 𠆞, 𠆟, 𠆠, 𠆡, 𠆢, 𠆣, 𠆤, 𠆥, 𠆦, 𠆧, 𠆨, 𠆩, 𠆪, 𠆫, 𠆬, 𠆭, 𠆮, 𠆯, 𠆰, 𠆱, 𠆲, 𠆳, 𠆴, 𠆵, 𠆶, 𠆷, 𠆸, 𠆹, 𠆺, 𠆻, 𠆼, 𠆽, 𠆾, 𠆿, 𠇀, 𠇁, 𠇂, 𠇃, 𠇄, 𠇅, 𠇆, 𠇇, 𠇈, 𠇉, 𠇊, 𠇋, 𠇌, 𠇍, 𠇎, 𠇏, 𠇐, 𠇑, 𠇒, 𠇓, 𠇔, 𠇕, 𠇖, 𠇗, 𠇘, 𠇙, 𠇚, 𠇛, 𠇜, 𠇝, 𠇞, 𠇟, 𠇠, 𠇡, 𠇢, 𠇣, 𠇤, 𠇥, 𠇦, 𠇧, 𠇨, 𠇩, 𠇪, 𠇫, 𠇬, 𠇭, 𠇮, 𠇯, 𠇰, 𠇱, 𠇲, 𠇳, 𠇴, 𠇵, 𠇶, 𠇷, 𠇸, 𠇹, 𠇺, 𠇻, 𠇼, 𠇽, 𠇾, 𠇿, 𠈀, 𠈁, 𠈂, 𠈃, 𠈄, 𠈅, 𠈆, 𠈇, 𠈈, 𠈉, 𠈊, 𠈋, 𠈌, 𠈍, 𠈎, 𠈏, 𠈐, 𠈑, 𠈒, 𠈓, 𠈔, 𠈕, 𠈖, 𠈗, 𠈘, 𠈙, 𠈚, 𠈛, 𠈜, 𠈝, 𠈞, 𠈟, 𠈠, 𠈡, 𠈢, 𠈣, 𠈤, 𠈥, 𠈦, 𠈧, 𠈨, 𠈩, 𠈪, 𠈫, 𠈬, 𠈭, 𠈮, 𠈯, 𠈰, 𠈱, 𠈲, 𠈳, 𠈴, 𠈵, 𠈶, 𠈷, 𠈸, 𠈹, 𠈺, 𠈻, 𠈼, 𠈽, 𠈾, 𠈿, 𠉀, 𠉁, 𠉂, 𠉃, 𠉄, 𠉅, 𠉆, 𠉇, 𠉈, 𠉉, 𠉊, 𠉋, 𠉌, 𠉍, 𠉎, 𠉏, 𠉐, 𠉑, 𠉒, 𠉓, 𠉔, 𠉕, 𠉖, 𠉗, 𠉘, 𠉙, 𠉚, 𠉛, 𠉜, 𠉝, 𠉞, 𠉟, 𠉠, 𠉡, 𠉢, 𠉣, 𠉤, 𠉥, 𠉦, 𠉧, 𠉨, 𠉩, 𠉪, 𠉫, 𠉬, 𠉭, 𠉮, 𠉯, 𠉰, 𠉱, 𠉲, 𠉳, 𠉴, 𠉵, 𠉶, 𠉷, 𠉸, 𠉹, 𠉺, 𠉻, 𠉼, 𠉽, 𠉾, 𠉿, 𠊀, 𠊁, 𠊂, 𠊃, 𠊄, 𠊅, 𠊆, 𠊇, 𠊈, 𠊉, 𠊊, 𠊋, 𠊌, 𠊍, 𠊎, 𠊏, 𠊐, 𠊑, 𠊒, 𠊓, 𠊔, 𠊕, 𠊖, 𠊗, 𠊘, 𠊙, 𠊚, 𠊛, 𠊜, 𠊝, 𠊞, 𠊟, 𠊠, 𠊡, 𠊢, 𠊣, 𠊤, 𠊥, 𠊦, 𠊧, 𠊨, 𠊩, 𠊪, 𠊫, 𠊬, 𠊭, 𠊮, 𠊯, 𠊰, 𠊱, 𠊲, 𠊳, 𠊴, 𠊵, 𠊶, 𠊷, 𠊸, 𠊹, 𠊺, 𠊻, 𠊼, 𠊽, 𠊾, 𠊿, 𠋀, 𠋁, 𠋂, 𠋃, 𠋄, 𠋅, 𠋆, 𠋇, 𠋈, 𠋉, 𠋊, 𠋋, 𠋌, 𠋍, 𠋎, 𠋏, 𠋐, 𠋑, 𠋒, 𠋓, 𠋔, 𠋕, 𠋖, 𠋗, 𠋘, 𠋙, 𠋚, 𠋛, 𠋜, 𠋝, 𠋞, 𠋟, 𠋠, 𠋡, 𠋢, 𠋣, 𠋤, 𠋥, 𠋦, 𠋧, 𠋨, 𠋩, 𠋪, 𠋫, 𠋬, 𠋭, 𠋮, 𠋯, 𠋰, 𠋱, 𠋲, 𠋳, 𠋴, 𠋵, 𠋶, 𠋷, 𠋸, 𠋹, 𠋺, 𠋻, 𠋼, 𠋽, 𠋾, 𠋿, 𠌀, 𠌁, 𠌂, 𠌃, 𠌄, 𠌅, 𠌆, 𠌇, 𠌈, 𠌉, 𠌊, 𠌋, 𠌌, 𠌍, 𠌎, 𠌏, 𠌐, 𠌑, 𠌒, 𠌓, 𠌔, 𠌕, 𠌖, 𠌗, 𠌘, 𠌙, 𠌚, 𠌛, 𠌜, 𠌝, 𠌞, 𠌟, 𠌠, 𠌡, 𠌢, 𠌣, 𠌤, 𠌥, 𠌦, 𠌧, 𠌨, 𠌩, 𠌪, 𠌫, 𠌬, 𠌭, 𠌮, 𠌯, 𠌰, 𠌱, 𠌲, 𠌳, 𠌴, 𠌵, 𠌶, 𠌷, 𠌸, 𠌹, 𠌺, 𠌻, 𠌼, 𠌽, 𠌾, 𠌿, 𠍀, 𠍁, 𠍂, 𠍃, 𠍄, 𠍅, 𠍆, 𠍇, 𠍈, 𠍉, 𠍊, 𠍋, 𠍌, 𠍍, 𠍎, 𠍏, 𠍐, 𠍑, 𠍒, 𠍓, 𠍔, 𠍕, 𠍖, 𠍗, 𠍘, 𠍙, 𠍚, 𠍛, 𠍜, 𠍝, 𠍞, 𠍟, 𠍠, 𠍡, 𠍢, 𠍣, 𠍤, 𠍥, 𠍦, 𠍧, 𠍨, 𠍩, 𠍪, 𠍫, 𠍬, 𠍭, 𠍮, 𠍯, 𠍰, 𠍱, 𠍲, 𠍳, 𠍴, 𠍵, 𠍶, 𠍷, 𠍸, 𠍹, 𠍺, 𠍻, 𠍼, 𠍽, 𠍾, 𠍿, 𠎀, 𠎁, 𠎂, 𠎃, 𠎄, 𠎅, 𠎆, 𠎇, 𠎈, 𠎉, 𠎊, 𠎋, 𠎌, 𠎍, 𠎎, 𠎏, 𠎐, 𠎑, 𠎒, 𠎓, 𠎔, 𠎕, 𠎖, 𠎗, 𠎘, 𠎙, 𠎚, 𠎛, 𠎜, 𠎝, 𠎞, 𠎟, 𠎠, 𠎡, 𠎢, 𠎣, 𠎤, 𠎥, 𠎦, 𠎧, 𠎨, 𠎩, 𠎪, 𠎫, 𠎬, 𠎭, 𠎮, 𠎯, 𠎰, 𠎱, 𠎲, 𠎳, 𠎴, 𠎵, 𠎶, 𠎷, 𠎸, 𠎹, 𠎺, 𠎻, 𠎼, 𠎽, 𠎾, 𠎿, 𠏀, 𠏁, 𠏂, 𠏃, 𠏄, 𠏅, 𠏆, 𠏇, 𠏈, 𠏉, 𠏊, 𠏋, 𠏌, 𠏍, 𠏎, 𠏏, 𠏐, 𠏑, 𠏒, 𠏓, 𠏔, 𠏕, 𠏖, 𠏗, 𠏘, 𠏙, 𠏚, 𠏛, 𠏜, 𠏝, 𠏞, 𠏟, 𠏠, 𠏡, 𠏢, 𠏣, 𠏤, 𠏥, 𠏦, 𠏧, 𠏨, 𠏩, 𠏪, 𠏫, 𠏬, 𠏭, 𠏮, 𠏯, 𠏰, 𠏱, 𠏲, 𠏳, 𠏴, 𠏵, 𠏶, 𠏷, 𠏸, 𠏹, 𠏺, 𠏻, 𠏼, 𠏽, 𠏾, 𠏿, 𠐀, 𠐁, 𠐂, 𠐃, 𠐄, 𠐅, 𠐆, 𠐇, 𠐈, 𠐉, 𠐊, 𠐋, 𠐌, 𠐍, 𠐎, 𠐏, 𠐐, 𠐑, 𠐒, 𠐓, 𠐔, 𠐕, 𠐖, 𠐗, 𠐘, 𠐙, 𠐚, 𠐛, 𠐜, 𠐝, 𠐞, 𠐟, 𠐠, 𠐡, 𠐢, 𠐣, 𠐤, 𠐥, 𠐦, 𠐧, 𠐨, 𠐩, 𠐪, 𠐫, 𠐬, 𠐭, 𠐮, 𠐯, 𠐰, 𠐱, 𠐲, 𠐳, 𠐴, 𠐵, 𠐶, 𠐷, 𠐸, 𠐹, 𠐺, 𠐻, 𠐼, 𠐽, 𠐾, 𠐿, 𠑀, 𠑁, 𠑂, 𠑃, 𠑄, 𠑅, 𠑆, 𠑇, 𠑈, 𠑉, 𠑊, 𠑋, 𠑌, 𠑍, 𠑎, 𠑏, 𠑐, 𠑑, 𠑒, 𠑓, 𠑔, 𠑕, 𠑖, 𠑗, 𠑘, 𠑙, 𠑚, 𠑛, 𠑜, 𠑝, 𠑞, 𠑟, 𠑠, 𠑡, 𠑢, 𠑣, 𠑤, 𠑥, 𠑦, 𠑧, 𠑨, 𠑩, 𠑪, 𠑫, 𠑬, 𠑭, 𠑮, 𠑯, 𠑰, 𠑱, 𠑲, 𠑳, 𠑴, 𠑵, 𠑶, 𠑷, 𠑸, 𠑹, 𠑺, 𠑻, 𠑼, 𠑽, 𠑾, 𠑿, 𠒀, 𠒁, 𠒂, 𠒃, 𠒄, 𠒅, 𠒆, 𠒇, 𠒈, 𠒉, 𠒊, 𠒋, 𠒌, 𠒍, 𠒎, 𠒏, 𠒐, 𠒑, 𠒒, 𠒓, 𠒔, 𠒕, 𠒖, 𠒗, 𠒘, 𠒙, 𠒚, 𠒛, 𠒜, 𠒝, 𠒞, 𠒟, 𠒠, 𠒡, 𠒢, 𠒣, 𠒤, 𠒥, 𠒦, 𠒧, 𠒨, 𠒩, 𠒪, 𠒫, 𠒬, 𠒭, 𠒮, 𠒯, 𠒰, 𠒱, 𠒲, 𠒳, 𠒴, 𠒵, 𠒶, 𠒷, 𠒸, 𠒹, 𠒺, 𠒻, 𠒼, 𠒽, 𠒾, 𠒿, 𠓀, 𠓁, 𠓂, 𠓃, 𠓄, 𠓅, 𠓆, 𠓇, 𠓈, 𠓉, 𠓊, 𠓋, 𠓌, 𠓍, 𠓎, 𠓏, 𠓐, 𠓑, 𠓒, 𠓓, 𠓔, 𠓕, 𠓖, 𠓗, 𠓘, 𠓙, 𠓚, 𠓛, 𠓜, 𠓝, 𠓞, 𠓟, 𠓠, 𠓡, 𠓢, 𠓣, 𠓤, 𠓥, 𠓦, 𠓧, 𠓨, 𠓩, 𠓪, 𠓫, 𠓬, 𠓭, 𠓮, 𠓯, 𠓰, 𠓱, 𠓲, 𠓳, 𠓴, 𠓵, 𠓶, 𠓷, 𠓸, 𠓹, 𠓺, 𠓻, 𠓼, 𠓽, 𠓾, 𠓿, 𠔀, 𠔁, 𠔂, 𠔃, 𠔄, 𠔅, 𠔆, 𠔇, 𠔈, 𠔉, 𠔊, 𠔋, 𠔌, 𠔍, 𠔎, 𠔏, 𠔐, 𠔑, 𠔒, 𠔓, 𠔔, 𠔕, 𠔖, 𠔗, 𠔘, 𠔙, 𠔚, 𠔛, 𠔜, 𠔝, 𠔞, 𠔟, 𠔠, 𠔡, 𠔢, 𠔣, 𠔤, 𠔥, 𠔦, 𠔧, 𠔨, 𠔩, 𠔪, 𠔫, 𠔬, 𠔭, 𠔮, 𠔯, 𠔰, 𠔱, 𠔲, 𠔳, 𠔴, 𠔵, 𠔶, 𠔷, 𠔸, 𠔹, 𠔺, 𠔻, 𠔼, 𠔽, 𠔾, 𠔿, 𠕀, 𠕁, 𠕂, 𠕃, 𠕄, 𠕅, 𠕆, 𠕇, 𠕈, 𠕉, 𠕊, 𠕋, 𠕌, 𠕍, 𠕎, 𠕏, 𠕐, 𠕑, 𠕒, 𠕓, 𠕔, 𠕕, 𠕖, 𠕗, 𠕘, 𠕙, 𠕚, 𠕛, 𠕜, 𠕝, 𠕞, 𠕟, 𠕠, 𠕡, 𠕢, 𠕣, 𠕤, 𠕥, 𠕦, 𠕧, 𠕨, 𠕩, 𠕪, 𠕫, 𠕬, 𠕭, 𠕮, 𠕯, 𠕰, 𠕱, 𠕲, 𠕳, 𠕴, 𠕵, 𠕶, 𠕷, 𠕸, 𠕹, 𠕺, 𠕻, 𠕼, 𠕽, 𠕾, 𠕿, 𠖀, 𠖁, 𠖂, 𠖃, 𠖄, 𠖅, 𠖆, 𠖇, 𠖈, 𠖉, 𠖊, 𠖋, 𠖌, 𠖍, 𠖎, 𠖏, 𠖐, 𠖑, 𠖒, 𠖓, 𠖔, 𠖕, 𠖖, 𠖗, 𠖘, 𠖙, 𠖚, 𠖛, 𠖜, 𠖝, 𠖞, 𠖟, 𠖠, 𠖡, 𠖢, 𠖣, 𠖤, 𠖥, 𠖦, 𠖧, 𠖨, 𠖩, 𠖪, 𠖫, 𠖬, 𠖭, 𠖮, 𠖯, 𠖰, 𠖱, 𠖲, 𠖳, 𠖴, 𠖵, 𠖶, 𠖷, 𠖸, 𠖹, 𠖺, 𠖻, 𠖼, 𠖽, 𠖾, 𠖿, 𠗀, 𠗁, 𠗂, 𠗃, 𠗄, 𠗅, 𠗆, 𠗇, 𠗈, 𠗉, 𠗊, 𠗋, 𠗌, 𠗍, 𠗎, 𠗏, 𠗐, 𠗑, 𠗒, 𠗓, 𠗔, 𠗕, 𠗖, 𠗗, 𠗘, 𠗙, 𠗚, 𠗛, 𠗜, 𠗝, 𠗞, 𠗟, 𠗠, 𠗡, 𠗢, 𠗣, 𠗤, 𠗥, 𠗦, 𠗧, 𠗨, 𠗩, 𠗪, 𠗫, 𠗬, 𠗭, 𠗮, 𠗯, 𠗰, 𠗱, 𠗲, 𠗳, 𠗴, 𠗵, 𠗶, 𠗷, 𠗸, 𠗹, 𠗺, 𠗻, 𠗼, 𠗽, 𠗾, 𠗿, 𠘀, 𠘁, 𠘂, 𠘃, 𠘄, 𠘅, 𠘆, 𠘇, 𠘈, 𠘉, 𠘊, 𠘋, 𠘌, 𠘍, 𠘎, 𠘏, 𠘐, 𠘑, 𠘒, 𠘓, 𠘔, 𠘕, 𠘖, 𠘗, 𠘘, 𠘙, 𠘚, 𠘛, 𠘜, 𠘝, 𠘞, 𠘟, 𠘠, 𠘡, 𠘢, 𠘣, 𠘤, 𠘥, 𠘦, 𠘧, 𠘨, 𠘩, 𠘪, 𠘫, 𠘬, 𠘭, 𠘮, 𠘯, 𠘰, 𠘱, 𠘲, 𠘳, 𠘴, 𠘵, 𠘶, 𠘷, 𠘸, 𠘹, 𠘺, 𠘻, 𠘼, 𠘽, 𠘾, 𠘿, 𠙀, 𠙁, 𠙂, 𠙃, 𠙄, 𠙅, 𠙆, 𠙇, 𠙈, 𠙉, 𠙊, 𠙋, 𠙌, 𠙍, 𠙎, 𠙏, 𠙐, 𠙑, 𠙒, 𠙓, 𠙔, 𠙕, 𠙖, 𠙗, 𠙘, 𠙙, 𠙚, 𠙛, 𠙜, 𠙝, 𠙞, 𠙟, 𠙠, 𠙡, 𠙢, 𠙣, 𠙤, 𠙥, 𠙦, 𠙧, 𠙨, 𠙩, 𠙪, 𠙫, 𠙬, 𠙭, 𠙮, 𠙯, 𠙰, 𠙱, 𠙲, 𠙳, 𠙴, 𠙵, 𠙶, 𠙷, 𠙸, 𠙹, 𠙺, 𠙻, 𠙼, 𠙽, 𠙾, 𠙿, 𠚀, 𠚁, 𠚂, 𠚃, 𠚄, 𠚅, 𠚆, 𠚇, 𠚈, 𠚉, 𠚊, 𠚋, 𠚌, 𠚍, 𠚎, 𠚏, 𠚐, 𠚑, 𠚒, 𠚓, 𠚔, 𠚕, 𠚖, 𠚗, 𠚘, 𠚙, 𠚚, 𠚛, 𠚜, 𠚝, 𠚞, 𠚟, 𠚠, 𠚡, 𠚢, 𠚣, 𠚤, 𠚥, 𠚦, 𠚧, 𠚨, 𠚩, 𠚪, 𠚫, 𠚬, 𠚭, 𠚮, 𠚯, 𠚰, 𠚱, 𠚲, 𠚳, 𠚴, 𠚵, 𠚶, 𠚷, 𠚸, 𠚹, 𠚺, 𠚻, 𠚼, 𠚽, 𠚾, 𠚿, 𠛀, 𠛁, 𠛂, 𠛃, 𠛄, 𠛅, 𠛆, 𠛇, 𠛈, 𠛉, 𠛊, 𠛋, 𠛌, 𠛍, 𠛎, 𠛏, 𠛐, 𠛑, 𠛒, 𠛓, 𠛔, 𠛕, 𠛖, 𠛗, 𠛘, 𠛙, 𠛚, 𠛛, 𠛜, 𠛝, 𠛞, 𠛟, 𠛠, 𠛡, 𠛢, 𠛣, 𠛤, 𠛥, 𠛦, 𠛧, 𠛨, 𠛩, 𠛪, 𠛫, 𠛬, 𠛭, 𠛮, 𠛯, 𠛰, 𠛱, 𠛲, 𠛳, 𠛴, 𠛵, 𠛶, 𠛷, 𠛸, 𠛹, 𠛺, 𠛻, 𠛼, 𠛽, 𠛾, 𠛿, 𠜀, 𠜁, 𠜂, 𠜃, 𠜄, 𠜅, 𠜆, 𠜇, 𠜈, 𠜉, 𠜊, 𠜋, 𠜌, 𠜍, 𠜎, 𠜏, 𠜐, 𠜑, 𠜒, 𠜓, 𠜔, 𠜕, 𠜖, 𠜗, 𠜘, 𠜙, 𠜚, 𠜛, 𠜜, 𠜝, 𠜞, 𠜟, 𠜠, 𠜡, 𠜢, 𠜣, 𠜤, 𠜥, 𠜦, 𠜧, 𠜨, 𠜩, 𠜪, 𠜫, 𠜬, 𠜭, 𠜮, 𠜯, 𠜰, 𠜱, 𠜲, 𠜳, 𠜴, 𠜵, 𠜶, 𠜷, 𠜸, 𠜹, 𠜺, 𠜻, 𠜼, 𠜽, 𠜾, 𠜿, 𠝀, 𠝁, 𠝂, 𠝃, 𠝄, 𠝅, 𠝆, 𠝇, 𠝈, 𠝉, 𠝊, 𠝋, 𠝌, 𠝍, 𠝎, 𠝏, 𠝐, 𠝑, 𠝒, 𠝓, 𠝔, 𠝕, 𠝖, 𠝗, 𠝘, 𠝙, 𠝚, 𠝛, 𠝜, 𠝝, 𠝞, 𠝟, 𠝠, 𠝡, 𠝢, 𠝣, 𠝤, 𠝥, 𠝦, 𠝧, 𠝨, 𠝩, 𠝪, 𠝫, 𠝬, 𠝭, 𠝮, 𠝯, 𠝰, 𠝱, 𠝲, 𠝳, 𠝴, 𠝵, 𠝶, 𠝷, 𠝸, 𠝹, 𠝺, 𠝻, 𠝼, 𠝽, 𠝾, 𠝿, 𠞀, 𠞁, 𠞂, 𠞃, 𠞄, 𠞅, 𠞆, 𠞇, 𠞈, 𠞉, 𠞊, 𠞋, 𠞌, 𠞍, 𠞎, 𠞏, 𠞐, 𠞑, 𠞒, 𠞓, 𠞔, 𠞕, 𠞖, 𠞗, 𠞘, 𠞙, 𠞚, 𠞛, 𠞜, 𠞝, 𠞞, 𠞟, 𠞠, 𠞡, 𠞢, 𠞣, 𠞤, 𠞥, 𠞦, 𠞧, 𠞨, 𠞩, 𠞪, 𠞫, 𠞬, 𠞭, 𠞮, 𠞯, 𠞰, 𠞱, 𠞲, 𠞳, 𠞴, 𠞵, 𠞶, 𠞷, 𠞸, 𠞹, 𠞺, 𠞻, 𠞼, 𠞽, 𠞾, 𠞿, 𠟀, 𠟁, 𠟂, 𠟃, 𠟄, 𠟅, 𠟆, 𠟇, 𠟈, 𠟉, 𠟊, 𠟋, 𠟌, 𠟍, 𠟎, 𠟏, 𠟐, 𠟑, 𠟒, 𠟓, 𠟔, 𠟕, 𠟖, 𠟗, 𠟘, 𠟙, 𠟚, 𠟛, 𠟜, 𠟝, 𠟞, 𠟟, 𠟠, 𠟡, 𠟢, 𠟣, 𠟤, 𠟥, 𠟦, 𠟧, 𠟨,

The following additional settings apply only in the Standard UI:

Table 263. Additional environment migration settings – Standard UI only	
Setting	Definition
Allow ObjectManager XML	Controls whether ObjectManager XML files can be imported through Administration > Import Configuration . The default is false. The Task Focused UI supports XML files.
Asynchronous Timeout	The timeout value (in seconds) for AJAX calls on environment migration pages. The default is 120.
Maximum String Items	Controls how many rows are displayed in the Review selected items box when exporting items with environment migration. The value can be any integer greater than zero. The default is 10000. Certain categories of items that can be exported with Environment Migration (such as Application Text) contain many tens of thousands of items. To reduce the page size and make browsers more responsive when reviewing these categories, you can set a limit on the number of items that are shown. When a limit is set you can still use the search feature to find items beyond the row limit.
Process Log Report Page Spec	The location of the Process Log Report page spec. The default is <code>/_cw_channels/Reporting/Hidden Reports/CommandCenter/Administrative Reports/Environment Migration/Process Log Report.pagespec</code>

The **ImportConfiguration** and **ExportConfiguration** application permissions are required to access environment migration for import and export. For details on these permissions, see [“Types of application permissions”](#) on page 91.

You must also have read and write permissions on the **Migration Documents** folder. You can see the folder by clicking  > **System Configuration > System Files**. Or, in the Standard UI, click **Administration > Manage System Files > Files**.

You might also need read and write permissions on other folders, depending on what you are importing and exporting.

For an overview of environment migration, see [Chapter 26, “Migrating OpenPages environments,”](#) on page 865.

Supported migration items

You can use the environment migration capability to move items between any two OpenPages environments that are using the same version and patch level of OpenPages.

The following information types are part of environment migration and, as such, you can export them by using **Export Configuration** and import them by using **Import Configuration**.

- Object Profiles
- Object Types
- Field Groups
- Field Definitions
- Application Text
- Object Text
- Error Text

- Filters
- Field Dependencies
- Dependency Picklists
- Object Type Relationships
- Rule Sets
- Settings
- Object Type Dimensions
- Recursive Object Levels
- Date Dimension Types
- Date Dimension Type Associations
- Rules (for IBM OpenPages Regulatory Compliance Management)
- Security Rules
- Views (in the Task Focused UI)
- Workflows (workflow definitions in GRC Workflow)
- Calculations (calculation definitions in GRC Calculations)
- Solutions (solution visualizations in the Task Focused UI)

Note: Solutions from pre-8.2 environments are displayed with -Legacy in the solution name, for example ORM-Legacy.

- Jobs (schedule definitions in the Scheduler)
- Themes (in the Task Focused UI)

The following supplemental information types can be exported by using ObjectManager and imported in XML format by using **Import Configuration**:

- System data (typically loaded during installation)
 - File types (for example, ppt, xls, doc)
 - Application permissions
 - Currencies
 - Reporting folders (channels)
 - Locales
- User-related information
 - Users and user groups
 - Group memberships
 - User associations to profiles
 - Role templates
 - Role assignments
 - Delegated administrators
- Instance data
 - Instance data (for example, risk and control objects and field values)
 - Parent and child relationships
- Other
 - Currency exchange rates

Important: You must use ObjectManager rather than the migration export and import tools in the user interface when you migrate field groups that contain four-byte characters as defined in the CJK Unified Ideographs EXTENSION-B Unicode Block Name, such as:

丈, 己, 子, 乙, 丑, 工,
鷄, 騰, 毓, 鰻, 鱧

For information about ObjectManager, see [Chapter 27, “The ObjectManager tool,”](#) on page 881.

The environment migration export process creates a file in the Java ARchive (JAR) format (referred to in this document as a migration file). The migration file is automatically saved to the repository.

The exported migration file is named in the `<export file name prefix>-env-mig-
<MMddYYkkmmss>` format; where:

- `<export file name prefix>` is the value of the **Export File Name Prefix** setting (see [“Settings that apply to environment migration”](#) on page 865), truncated if the prefix exceeds 15 characters;
- the timestamp portion of the file name represents the month (MM), the day (dd), the year (YY), hour (kk), minute (mm), and seconds (ss) when the export was started.

For example, `openpages-env-mig-011712031416`.

Exporting dependencies

When you export certain configuration items, the export process automatically determines if there are any dependencies required by the configuration items and adds those dependencies to the migration file.

The dependencies that are exported for each type of item are listed in the following table.

Table 264. Dependent items exported	
Item	These dependencies are exported
Object profile	• views • object types (including all object type dependencies) • field groups (including all field group dependencies) • view labels • dashboards (in the Task Focused UI)
Object type	• field groups (including any underlying fields) • field dependencies • dependent picklists • filters • root folders • object type images • corresponding settings and object strings • object type relationships • file types (if the object type is file-upload based)
Field group	Any underlying fields
Application strings	Any corresponding string keys
Object type dimensions	Any recursive object levels, if associated

Table 264. Dependent items exported (continued)	
Item	These dependencies are exported
Date dimension type associations	Any corresponding date dimension types

Items that are not migrated

The following items are not exported by the environment migration tools. These items are not available for import into a target environment and the validation process does not identify these items as missing.

If any of the items that you plan to migrate has a dependency on one or more of these items, you need to move the dependent item or items manually prior to using the environment migration tools. For help determining if any dependencies will not be migrated and how to move those dependencies manually, contact IBM OpenPages Support.

Configuration settings that are not migrated

The configuration settings listed in [Table 265 on page 869](#), are not migrated by the environment migration tools.

Important: Do not to change the security model with the **Settings > Common > Security > Model** setting on the source system if there is instance data in the target system. If you do, the configuration settings import will fail.

Note: If the **Show Hidden Settings** setting is set to false, hidden settings are not migrated. For more information, see [“Show hidden settings” on page 602](#). To migrate hidden settings, set the **Show Hidden Settings** setting to true.

For example, if you export all settings, the settings in this table are not included in the exported JAR file.

Table 265. Configuration settings that are not exported	
Setting description	Location
Mail server name	Applications > Common > Email > Mail Server
SMTP user name	Applications > Common > Email > SMTP User Name
SMTP password	Applications > Common > Email > SMTP Password
SMTP security type	Applications > Common > Email > SMTP Security Type
SMTP port number	Applications > Common > Email > SMTP Port
SOCKS Proxy private IP address	Applications > Common > Email > SOCKS Proxy Private IP Address
Guest password on server	Platform > Application Server Guest Password
JMS listener Urls for all paired servers	Platform > Global Caches > JMS > Listener Urls
Default OpenPages e-mail sender address	Platform > Publishing > Mail > From Address
Default OpenPages e-mail server	Platform > Publishing > Mail > Host
Default OpenPages e-mail username	Platform > Publishing > Mail > Username

Table 265. Configuration settings that are not exported (continued)

Setting description	Location
OpenPages detail page name for reference by reporting tool	Platform > Reporting Schema > Object URL Generator > Detail Page
OpenPages server name for reference by reporting tool	Platform > Reporting Schema > Object URL Generator > Host
OpenPages server port for reference by reporting tool	Platform > Reporting Schema > Object URL Generator > Port
OpenPages application protocol for reference by reporting tool	Platform > Reporting Schema > Object URL Generator > Protocol
Export File Name Prefix	Applications > GRCM > Environment Migration > Export File Name Prefix
Index search server URL	Platform > Search > Index > Search Server URL
Request search server URL	Platform > Search > Request > Search Server URL
Search server administration URL	Platform > Search > Admin > Search Server Administration URL
Solr user ID	Platform > Search > Solr User ID
Solr password	Platform > Search > Solr Password

Metadata items not migrated

The following metadata items are not migrated by the environment migration tools. If any of these items is not in the target environment, you need to move the items manually.

- Triggers
- Custom query subjects
- JSPs
- Role templates
- Instance data

Although role templates and instance data are not part of the environment migration JAR files, you can migrate them by exporting them with ObjectManager and then importing the XML files with **Import Configuration**.

For the other items, such as JSPs, you need to copy the files from one environment to the other.

User security not migrated

User security is not migrated by the environment migration tools.

If there are profiles in the system containing user fields that have been scoped to specific security domain groups, verify that the same security domain groups are in place in the target environment. If not, configure the target environment to match the source.

The import validation process stops the import if any required security domain group is not present in the target environment. An error in the following format is displayed in the validation Log Details report:

```
<line#> Processing 'displayTypePropertyValue', Attribute: 'name', Value:
'<group Name>' is not defined in the migration package or in the target
system!: Group Missing!
```


User fields can have a scope defined that filters the amount of returned search data. This scope definition is based on security domain groups in the OpenPages with Watson environment. However, these security groups are not migrated by the environment migration.

If a user field has a scope defined in the source environment, but that configuration does not exist in the target environment, the import will be stopped.

For more information on setting the scope definitions, see [“Configure user and group selectors display types for simple strings \(Standard UI\)” on page 353](#).

Reports not migrated

Reports are not migrated by the environment migration tools.

If a profile contains an embedded report that is not available in the target environment, a user with that profile sees a message in the OpenPages with Watson interface that the report is missing.

Important: If you want a user to access an embedded report that is not present in the target environment, you must move the report manually from the source environment to the target environment before migrating the environment.

Item dependencies not migrated by default

Environment migration automatically determines if there are any dependencies required by the exported items and adds those dependencies to the migration file.

However, some items that can be exported for migration are not included automatically as dependencies.

The following metadata items are not exported as a dependency:

- Namespaces

If a profile includes a computed field that relies on a namespace, and that namespace does not exist (or is defined differently) in the target environment, the profile passes import validation. However, a user will not be able to access the computed field in the target environment. To avoid this scenario, ensure that all namespaces upon which computed fields have a dependency are included in the migration file.

- Objects, field groups, and fields

If a filter includes criteria that rely on an object, a field group, or a field that is not already in the target environment, the migration fails. To avoid this scenario, ensure that all objects, field groups, and fields upon which filters have a dependency are included in the migration file.

- Workflows that are used in IBM OpenPages Regulatory Compliance Management rules

When you export rules that you created in the **Rules Engine**, the export does not include the workflows that the rules trigger. For example, suppose you have a rule that is called Change Notification that triggers the Send Email Notification workflow. When you export rules, the Send Email Notification workflow is not included in the export. To migrate rules, you need to migrate both rules and their workflows to the target environment.

- Job dependencies

When you export jobs, the export does not include any dependencies, such as workflows or Java classes that the jobs trigger. For example, suppose you have a job that runs the BC Plan Review and Approval workflow. When you export the job, the workflow is not included in the export. To migrate jobs, you need to migrate both jobs and their workflows or Java classes to the target environment.

- Workflow dependencies

When you export workflows, the export does not include dependencies, such as views, object types, and custom actions. To migrate workflows, you need to migrate the workflows and their dependencies to the target environment. For more information, see [“Exporting and importing workflow definitions” on page 548](#).

- Calculation dependencies

When you export calculations, the export does not include any dependencies. To migrate calculations, you need to migrate the calculations and their dependencies to the target environment.

Environment migration best practices

When you use environment migration to move metadata and configuration items from one environment to another, use the following best practice guidelines to help ensure a smooth transition of information:

- A setting cannot be imported if the target system does not have the dependencies specified in the setting's value. To migrate the setting, first migrate the dependencies (such as object types, field groups, and recursive object levels) without the setting. Then, migrate the setting by using a separate migration file.
- Before you import security rules, you must import the metadata and create the reporting schema in the target environment.
- Import configuration items during planned downtime, when end users are not accessing that environment. Issues can arise if an end user is working with an item while that item is being imported.
- Replicate the metadata in your production environment to the development and/or test environment where you will be making and testing configuration changes.

Using the same configuration data in all environments ensures that:

- All environments operate on the same baseline set of OpenPages metadata as a starting point.
- Any test configurations or items in a test or development environment are removed, preventing those items from being migrated inadvertently to the production environment.

For more information about replicating environments, see [“The OPBackup utility”](#) on page 682.

- Make modifications and additions to configuration items in a test or development environment. After the items are tested, migrate the items to the production environment.
- If you are importing an XML file, you must use the ObjectManager loader file naming convention:

```
<loader-file-prefix>-op-config.xml
```

For more information about the naming convention, see [“Working with loader files”](#) on page 881.

- Before you import configuration items, validate the migration file. See [“Validating a migration file”](#) on page 876.
- If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before you submit another configuration job.
- If you migrate filters for large text fields, you must enable the text feature in your target database so that large text fields display correctly in the filters.

For more information about enabling the IBM Db2 Text Search feature, see [“Enable Db2 text search”](#) on page 702.

For more information about enabling the Oracle Text feature, see [“Enabling Oracle Text”](#) on page 748.

- When you import calculations, the import might fail if your target environment has calculation definitions. The issue occurs when there are input or output field conflicts on an object type. To resolve the issue, disable the existing calculations in your target environment, and then import the calculations again.

The environment migration process

From a single client system, you can use the OpenPages application to select and export changed configuration items in an OpenPages environment (the source), and then import them into another environment (the target). The environment migration import process automatically validates the imported items to ensure they will work properly in the target environment.

Table 266 on page 873 outlines the process for migrating configuration items from a source environment to a target environment by using the environment migration tools.

Table 266. Tasks for migrating items by using Environment Migration

Use this environment...	To do this task...
Source	Export the configuration items into a migration file. See “Exporting configuration items from the source environment (Task Focused UI)” on page 873 or “Exporting configuration items from the source environment (Standard UI)” on page 874.
Target	Import the configuration items into the target environment. See “Importing configuration items to the target environment” on page 875.

Exporting configuration items from the source environment (Task Focused UI)

You can export configuration items. The export process creates a JAR file, which is automatically saved to the repository. You can also download the migration file to save it locally.

Important:

- If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before submitting another configuration job.
- You cannot export while in System Admin Mode (SAM). For more information, see [Chapter 3, “System Admin Mode \(SAM\),”](#) on page 71.
- The export will fail if you have invalid triggers. Disable triggers before you export.

Before you begin

You must be logged in as an OpenPages administrator who has the **ExportConfiguration** application permission. You must also have read and write access to the **Migration Documents** folder. For more information, see [“Types of application permissions”](#) on page 91.

The export will fail if you have invalid triggers. Disable triggers before you export.

About this task

If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before submitting another configuration job.

You cannot export while in System Admin Mode (SAM). For more information, see [Chapter 3, “System Admin Mode \(SAM\),”](#) on page 71.

Procedure

1. Log on to the source OpenPages application as an administrator.
2. Disable System Admin Mode, if it is enabled. For more information, see [“Enabling and disabling System Admin Mode”](#) on page 71.
3. If you want to migrate hidden settings, set **Show Hidden Settings** to true.
4. Click  > **System Migration** > **Export Configuration**.
5. Click **Add Items**.
6. Select the items that you want to export, and then click **Select**.
For example, if you want to export profiles, click **Object Profiles** and then select the profiles that you want to export.

You can select items from multiple categories.
7. Review the list of selected items. If you want to change them, click **Edit Selections**.
8. Click **Save Migration File**.

The items are exported to a migration file in JAR format.

The migration file is saved to the **Migration Documents** folder in the repository.

9. Optional: To download the migration file to your local system, click **Download**.

Exporting configuration items from the source environment (Standard UI)

You can create a new migration file each time you perform an export or you can add additional items to an existing migration file. The migration file is automatically saved to the repository and can optionally be saved to a local client.

Important:

- If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before submitting another configuration job.
- You cannot export while in System Admin Mode (SAM). For more information, see [Chapter 3, “System Admin Mode \(SAM\),”](#) on page 71.
- The export will fail if you have invalid triggers. Disable triggers prior to doing the export configuration.

Before you begin

You must be logged in as an OpenPages administrator who has the **ExportConfiguration** application permission. You must also have read and write access to the **Migration Documents** folder. For more information, see [“Types of application permissions”](#) on page 91.

Procedure

1. Log on to the source OpenPages application as an administrator.
2. Disable System Admin Mode, if it is enabled. For more information, see [“Enabling and disabling System Admin Mode”](#) on page 71.
3. From the menu bar, click **Administration > Export Configuration**.
4. On the **Export Options** tab, do one of the following:
 - a) Under **Create a new migration package**, select **Export local configuration** to create a new migration file and click **Submit**.
 - b) Under **Create new export based on a previously saved migration package (JAR)** select either **Local disk** or **Server repository**. Click the **Browse** icon to locate the migration file to use, then click **Submit**.

Note: If you selected the wrong package, reload the **Export Configuration** page or click the browser's **Back** icon.

5. In the **Choose items to export** tab, select the type of item to export from the **Choose type** drop-down list.
6. In the **Select items** pane, use the list or the tree structure to select specific items to export or click **All** to select all the items of that type. Click **None** to clear the list of selected items.

The **Review items** pane displays the current count of each type.

7. Repeat Steps 5 and 6 for each type of item you want to export.
8. Optional: To review the details of the selected items, click the links in the **Review selected items** pane. All items of that type selected for export are displayed in the **Selected item details** pane.
9. Click the **Clear** icon to remove the items from the display. Clearing the list will not remove the items from the file.

To remove an item from the migration file, select the type of item to remove from the **Choose type** drop-down list. Locate the item(s) in the list or the tree structure and clear the check box.

10. When you have selected the objects to export, click the **Save migration file** icon.

The **Export History** pane shows the progress of the export.

View a detailed status by clicking the **View Log** icon to launch the Log Summary report. This report shows the number of items that have been logged in the Process Log Report, under the **Full system detail log** link. See [“Log summary migration report \(Standard UI\)”](#) on page 879 and [“Log details migration report \(Standard UI\)”](#) on page 880.

11. Click the **Refresh** icon in the **Export History** pane to update the progress on screen in real-time. When the export is complete, the **Export History** pane will display a message indicating if the export completed successfully or with errors. If successful, the migration file is saved to the OpenPages repository. If the Completed With Errors message appears, you can use the migration reports to determine the nature of the error.

The **Export Configuration** page returns to the initial state, allowing you to perform additional exports, as needed.

Importing configuration items to the target environment

You can load the migration file into the target environment by downloading the file from the OpenPages repository or by importing a saved file from your local client.

The import process automatically validates the configuration items before performing the import to ensure that the items are complete and any object dependencies are in the migration file or in the target environment before the items are imported. The validation process verifies that:

- The XML file is a well-formed ObjectManager loader file.
- The metadata attributes are valid, according to the OpenPages validation rules.
- All dependent items that a particular item requires are present in either in the migration file or in the target system.
- Special characters are validated if the **Special Character Validation** setting is true (see [“Settings that apply to environment migration”](#) on page 865).

You can also run the validation process separately from the import. See [“Validating a migration file”](#) on page 876.

To avoid validation errors, review the information on dependent items that must be manually created and/or moved to the target environment. For details, see [“Items that are not migrated”](#) on page 869. For example, if you select a filter for import, ensure that all objects, field groups, and fields that are used by the filter are either included in the migration file or already in the target system.

You must have the **ImportConfiguration** application permission. You must also have read and write access to the **Migration Documents** folder. For information, see [“Types of application permissions”](#) on page 91 and [“Managing system files and folders \(Task Focused UI\)”](#) on page 191.

Important: The environment migration import process might periodically enable System Admin Mode (SAM), preventing users from making and saving changes (see [“Enabling and disabling System Admin Mode”](#) on page 71). To avoid errors in the imported data and other issues, migrate data during off-hours or when the target environment is not being used.

Configuring environment migration to allow special characters

The environment migration import process checks for any special characters in the name of the items being imported. By default, if any item has a name with a special character, the import stops. To import metadata items that use special characters in their names, you must disable this validation.

Procedure

1. Access the **Settings** page (see [Chapter 19, “Viewing the Configuration and Settings page,”](#) on page 597).
2. Go to the **Applications > GRCM > Environment Migration > Special Character Validation** setting.
3. In the **Value** box, type one of the following values:

If the value is set to...	Then...
true	The import process checks for special characters in the name of metadata items being imported. This value is the default.
false	The import process allows metadata items with special characters in the name to be imported.

4. Click **Done**.

Validating a migration file

This task is optional. The import process validates migration files automatically, but you can also run a validation separately from an import.

Important: If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before submitting another configuration job.

If you are importing an XML format file, you must use the following file naming convention:

```
<loader-file-prefix>-op-config.xml
```

Validating a migration file in the Task Focused UI

Procedure

1. Log on to the target OpenPages application as a user with the **Import Configuration** permission.
2. Click  > **System Migration** > **Import Configuration**.
3. Select the migration file.
 - If the migration file is on your local system, click **Local drive**, and then click **Add file**.
 - If the migration file is in the repository, click **Server repository**, and then click the file that you want to validate.
4. Click **Validate**.

Results

If The requested operation could not be completed is displayed, check the migration file. The file must be either a migration JAR file or an ObjectManager XML file.

If Completed With Errors is displayed, review the status messages on the **History** tab for information about the errors. You must fix validation errors before you import the migration file.

Validating a migration file in the Standard UI

Procedure

1. Log on to the target IBM OpenPages with Watson application as a user with the **Import Configuration** permission.
2. From the menu bar, select **Administration** > **Import Configuration**.
3. On the **Import Options** tab, select one of the following based on where the migration file is located:
 - a) **Local Disk** to import a file from the local machine. The migration file can be in either JAR or XML format.
 - b) **Server repository** to import a migration file from the OpenPages with Watson repository. Click **Browse** to locate the migration file to import.

4. Click **Submit**.
5. To review the details of the selected items, click the links in the **Review items in the migration package** pane. If you are importing a JAR format file, all items of that type selected for import are displayed in the **Selected item details** pane. If you are importing an XML format file, supplemental information types are validated but not displayed in the **Selected item details** pane. For more information about, see [“Supported migration items” on page 866](#).

Click **Clear** to remove the items from the display. Clearing the list will not remove the items from the file.

Note: If you selected the wrong migration file, reload the **Import Configuration** page or click **Back** in the browser.

6. Click **Validate** to begin the validation process.
The **Import History** pane shows the progress of the validation. You can view a detailed status by clicking **View Log**.
7. Click **Refresh** in the **Import History** pane to update the progress on screen. When the validation is complete, the **Import History** pane will display a message indicating if the validation completed successfully or with errors.

Results

If the **Completed With Errors** message appears, you can use the migration reports to determine the nature of the error. See [“Log summary migration report \(Standard UI\)” on page 879](#) and [“Log details migration report \(Standard UI\)” on page 880](#). If there are any validation errors, these errors will need to be addressed before importing.

If there are warnings in the migration reports, these can be safely ignored, and you can continue with the import.

Importing a migration file (Task Focused UI)

Use the following instructions to import configuration changes by using **Import Configuration**.

Important: Do not manually make changes to the application configuration during the import. Doing this can corrupt the data or result in errors. If this occurs, you must re-export the data before you attempt the import again.

Before you begin

- If an import, export, or validate process is currently running on the system, you must wait until processing is complete before you submit another import, export, or validate job.
- The source and target environments must have the same version and patch level of OpenPages.
- Ensure that any dependencies that are not included in the migration file are imported first. For example, if you are migrating profiles and the profiles use embedded reports on the home page, import the reports manually before you import the profiles.
- On the target system, check the value of the **Applications > GRCM > Home Page > Maximum Reports Listing** setting. This setting must have a value that is equal to, or greater than, the value for this setting in the source system. For information about how to access the Settings page, see [Chapter 19, “Viewing the Configuration and Settings page,” on page 597](#).

Procedure

1. Log on to the target OpenPages application as a user with the **ImportConfiguration** permission and read and write to the **Migration Documents** folder.
2. Click  > **System Migration > Import Configuration**.
3. Select the migration file (.jar or .xml).
 - If the migration file is on your local system, click **Local drive**, and then click **Add file**.

- If the migration file is in the repository, click **Server repository**, and then click the file that you want to import.

The **Review Items** pane shows the items that will be imported, if those items are supported by the environment migration user interface. If you are importing other items, such as role templates, the items are not displayed, but they are imported. For more information, see [“Supported migration items” on page 866](#).

4. Click **Import**.

Results

If The requested operation could not be completed is displayed, check the migration file. The file must be either a migration JAR file or an ObjectManager XML file.

If Completed With Errors is displayed, review the status messages on the **History** tab for information about the errors and review the [“Environment migration best practices” on page 872](#). You must fix the errors before you import the migration file.

Importing a migration file (Standard UI)

Use the following instructions to import configuration changes by using **Administration > Import Configuration**.

Important: Do not manually make changes to the application configuration during the import. This can corrupt the data or result in errors. In either case, you must re-export the data before attempting the import again. If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before submitting another configuration job.

Before you begin

- The source and target environments must have the same version and patch level of OpenPages with Watson.
- If the profiles that are being exported have home page report tabs, or report listings in the classic tab configured, then those reports have to be manually imported into the target system first, since environment migration does not support reports.
- On the target system, check the value of the **Applications > GRCM > Home Page > Maximum Reports Listing** setting. This setting must have a value that is equal to, or greater than, the value for this setting in the source system. For instructions on accessing the settings page, see [Chapter 19, “Viewing the Configuration and Settings page,” on page 597](#).

Procedure

1. Log on to the target IBM OpenPages with Watson application as a user with the **ImportConfiguration** permission and access to the **Migration Documents** folder.
2. From the menu bar, select **Administration > Import Configuration**.
3. On the **Import Options** tab, select one of the following, based on where the migration file is located:
 - a) **Local Disk** to import a file from the local machine. The migration file can be in either JAR or XML format.
 - b) **Server repository** to import a file from the OpenPages repository. Click **Browse** to locate the migration file to import.
4. Click **Submit**.
5. To review the details of the selected items, click the links in the **Review items in migration package** pane. If you are importing a JAR file, all items of that type selected for import are displayed in the **Selected item details** pane. If you are importing an XML file, supplemental information types are validated but not displayed in the **Selected item details** pane. For more information, see [“Supported migration items” on page 866](#).

Click **Clear** to remove the items from the display. Clearing the list will not remove the items from the file.

Note: If you selected the wrong migration file, reload the **Import Configuration** page or click **Back** in the browser.

6. When you are satisfied with the data to import, click **Import**. The environment migration process automatically validates the data before importing.

The process will either:

- Import the data, if there are no validation errors;
- Stop the import if there are validation errors. If there are errors that need to be corrected, see [“Environment migration best practices” on page 872](#).

The **Import History** pane shows the progress of the import. You can view a detailed status, by clicking **View Log**.

7. Click **Refresh** in the **Import History** pane to update the progress on screen. When the import is complete, the **Import History** pane will display a message indicating if the import completed successfully or with errors. If the Completed With Errors message appears, you can use the migration reports to determine the nature of the error. See [“Log summary migration report \(Standard UI\)” on page 879](#) and [“Log details migration report \(Standard UI\)” on page 880](#).

The **Import Configuration** page returns to the initial state, allowing you to perform additional imports, as needed.

Results

- After the import, you can click **View Log** to download a report with feedback on the current status, number of correctly validated items, and any inconsistencies or failed validations.

Note: After importing a migration file, the file is added to the repository. The name of the file includes the end time of the import in the <export file name prefix>-<YYYY_MM_dd_kk_mm> format. If you need to import the migration file into another system, use the exported migration file.

For example, suppose the **Import History** window indicates that the migration file migration-100311120839 was imported. The repository shows that migration-100411031232.jar was created. If you need to import this package of changes into another system, select the migration-100311120839.jar file. (The name indicates that the value of the Export File Name Prefix setting is migration.)

- If you imported profiles, update the reporting schema. For more information, see [“Updating the reporting schema” on page 162](#).
- If, as part of the import, updates are made to the **Platform > Reporting Framework V6 > Configuration > Supported Triangle Relationships** setting, you must recreate the reporting schema to update it with the new triangle views. For instructions, see [“Changes that require the reporting schema to be updated or recreated” on page 159](#).

Log summary migration report (Standard UI)

To view a summary report, click the **View Log** icon next to any ongoing or complete migration process in the **History** pane. The Log Summary report is a report that lists the status of the items in the process.

For exports, only the **Full System Detail Log** is generated.

The Log Summary report contains the following status fields:

- **Successes.** The number of items that were validated or imported without error. Click the link to view further details on the successfully processed items.
- **Warnings.** The number of items that resulted in a warning. Click the link to view further details on the warnings. If there are warnings, these can be safely ignored. They will not affect the processing.
- **Failures.** The number of items that resulted in some error. Click the link to view further details on the items that failed during the validation.

- **Overall Items Processed.** The total number of items validated or imported.
- **Full System Detail Log.** The number of items recorded in the Log Details report.

When a validation or an import encounters warnings and/or failures, the description of the message usually indicates how to correct the problem.

For example, if an attribute is missing or an item is missing a parent dependency, you need to correct the issue on the source system and export the file again. Or, you can contact IBM OpenPages Support for assistance.

Log details migration report (Standard UI)

During or after an export, validation, or import process has run, click the **Full System Detail Log** link in the Log Summary report to view details about the process. The information in the report depends upon the process being performed:

- **Export.** When exporting, the Log Details report lists the items exported and an overview of the number and type of items exported.
- **Validation.** When validating, the Log Details report lists the items being validated and whether the item is valid or there is an error.
- **Import.** When importing, the Log Details report first provides information about the validation process, listing the items being validated and whether the item is valid or there is an error. If the validation succeeds, the report provides information on the import process, listing the items imported and an overview of the number and types of items imported.

Chapter 27. The ObjectManager tool

The ObjectManager tool provides a command-line interface (CLI) that you can use instead of the application graphical user interface to load data into the IBM OpenPages with Watson repository.

With the ObjectManager tool, you can perform the following tasks:

- Import (load) data, such as objects and configuration data, into the OpenPages with Watson repository.
- Export (dump) filtered or unfiltered data from the OpenPages with Watson repository. You can use this functionality, for example, to migrate environments and data from one computer to another one in a multi-deployment environment.
- Batch-load multiple loader files in a single session.

Only a Super Administrator has full access to ObjectManager operations.

If you use ObjectManager to load data from one environment into another, the source and target environments must have the same version and patch level of OpenPages with Watson.

An alternative to using the ObjectManager tool is to use **Administration > Import Configuration** in the Standard UI. You can use it to load system data, user-related information, and instance data. The rules that apply to loader files that are imported with the ObjectManager tool apply also to **Import Configuration**.

The ability to import ObjectManager XML files through **Import Configuration** is controlled by the Applications/GRCM/Environment Migration/Allow ObjectManager XML registry setting. It is disabled by default.

You can change the ObjectManager configuration settings, such as the maximum size of requests that are sent from ObjectManager to the REST API. For more information, see [“Tools properties and parameters ” on page 1085](#).

Working with loader files

The ObjectManager tool uses XML loader files to load (import) or dump (export or extract) data into IBM OpenPages with Watson.

The loader file name consists of a prefix, which is defined by the user, and a standard string that has the following format:

```
<loader-file-prefix>-op-config.xml
```

Where:

- <loader-file-prefix> is the user-defined portion of the loader file name.
- -op-config.xml is the standard string that follows the prefix and identifies the file as a loader file to the ObjectManager tool. Do not change this portion of the file name.

When you pass a loader file parameter to the ObjectManager tool, you pass only the prefix portion of the loader file name. If no prefix is provided, the ObjectManager tool attempts to load from or write to the file op-config.xml.

Note: If you use ObjectManager to import security rules, any existing security rules are overwritten by the import.

Import example

If you want to load (import) data into the OpenPages with Watson repository, you could, for example, create a loader file with the name mydata-op-config.xml (prefix + standard string). When you pass the prefix mydata to the ObjectManager tool, the ObjectManager tool automatically looks for a loader file that is named mydata-op-config.xml.

Export example

If you want to extract (dump) data from OpenPages with Watson, you could, for example, pass the prefix `myconfig` to the ObjectManager tool. The ObjectManager tool automatically creates an export (dump) file that is named `myconfig-op-config.xml`.

Creating a data loader file

A data loader file is an XML file that contains the data you want to import or load through the ObjectManager into your system.

You can use any XML or text editor of your choice to create a data loader file.

After you create the data loader file, save it using the file naming convention described in [“Working with loader files”](#) on page 881.

All element tags in a data loader file are nested within the root element `<openpagesConfiguration xmlFormatVersion="1.31">` and `</openpagesConfiguration>` tags.

An ObjectManager data loader file has the following structure:

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
  <parent-element>
    <child-element/>
    <child-element/>
  </parent-element>
</openpagesConfiguration>
```

Where:

`parent-element` is a tag identifying the type of information to be loaded.

`child-element` is a nested tag within a given information type that usually contains attributes and/or text content.

The following code example shows the structure of an XML data loader file that, when loaded through the ObjectManager tool, updates the currency exchange rates for the Canadian dollar (CAD) and Mexican peso (MXN).

The `exchangeRates` element contains the `exchangeRate` child-element, which has attributes for the 3-letter ISO code for the country or region and the updated exchange rate for that currency. The rate can use up to eight decimal places.

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
  <exchangeRates>
    <exchangeRate isoCode="CAD"
      startDate="2020-05-09 17:36:12"
      rate="0.8636"/>
    <exchangeRate isoCode="MXN"
      startDate="2020-05-09 17:36:12"
      rate="0.0951"/>
  </exchangeRates>
</openpagesConfiguration>
```

Running ObjectManager commands

The ObjectManager command file is named `ObjectManager.cmd` on computers running a Microsoft Windows operating system. The command file is named `ObjectManager.sh` on computers running a Linux operating system.

The file is located in the `<OP_HOME>/bin` directory on OpenPages with Watson application servers.

Table 267. Installation location of the OpenPages with Watson application

Operating system	Installation location
Windows	For example, <OP_Home> C:\IBM\OpenPages
Linux	For example, <OP_Home> /opt/IBM/OpenPages

Tip: You can also run ObjectManager from a remote system, such as your laptop. For more information, see [“Installing tools and utilities \(IBM OpenPages with Watson\)”](#) on page 824

The ObjectManager command line must be:

- Run from the bin folder
- Typed on a single line (no line breaks) in a command window.

Important: When using the ObjectManager tool, make sure that the OpenPages with Watson application services are running.

Interactive command line loader file syntax

The ObjectManager tool uses the following syntax for a loader file.

Note: Make sure to run the command on a single line in the Command Prompt window.

```
ObjectManager <command> config|c <user> <password> <loader-file-path> <loader-file-prefix>
```

ObjectManager command line parameters

You can use various commands and parameters with the ObjectManager tool.

<command>

Required.

Value can be one of the following:

- dump or d - dumps or exports data.
- load or l - loads or imports data from a single loader file.
- validate or v - certifies or compares data.

<batch-mode>

Places ObjectManager in batch processing mode. Loads multiple loader files in a single session.

Value is batch or b.

For more information, see [“Batch loader file syntax and sample”](#) on page 885.

<user> and <password>

Required.

Some actions may require a Super Administrator account.

Both parameters are used for authentication. You can use your user ID and your password.

When you are running ObjectManager for OpenPages version 8.2.0.3 or later on Cloud Pak for Data, use one of the following combinations instead of your user ID and password:

- jwt and a Cloud Pak for Data JSON Web Token (JWT)
- your Cloud Pak for Data user name and your Cloud Pak for Data API key

An API Key can be generated in Cloud Pak for Data. For more information, see [Generating API keys for authentication](#).

To see examples of using these parameters in IBM OpenPages for IBM Cloud Pak for Data, see [“Load command example”](#) on page 884.

<loader-file-path>

Optional.

The file path to a single XML loader file.

By default, this is the current directory if no file path is specified.

The `ObjectManager.log` file is written to this directory.

<batch-loader-dir>

Optional.

The directory path to the XML loader files that are listed in the `<batch-loader-list-file>`. Can be a top-level directory if loader files are in multiple sub-folders under that directory.

<loader-file-prefix>

Optional.

The user-defined portion of the loader file name.

By default, the ObjectManager tool attempts to load from or write to the file `op-config.xml`, if no prefix is specified.

<batch-loader-list-file>

Required.

The fully qualified file path and name of a text document containing a list of loader files for batch processing.

Load command example

This Windows-based example shows how to use a loader file that is named `data1-op-config.xml` that resides in the `c:\import` folder to load or import data into IBM OpenPages with Watson.

This example uses the Super Administrator account, `OpenPagesAdministrator`.

Procedure

1. Open a Command Prompt window.
2. Navigate to the bin installation directory, such as:

```
cd C:\OpenPages\bin
```

3. Run the following command on a single line to load the `data1-op-config.xml` loader file:

```
ObjectManager l c OpenPagesAdministrator OpenPagesAdministrator c:\import data1
```

The log file is `c:\import\ObjectManager.log`.

If you are running ObjectManager for OpenPages version 8.2.0.3 or later on Cloud Pak for Data, use one of the following options for specifying the user name and password in a command:

- Use `jwt` and a Cloud Pak for Data JSON Web Token (JWT) as in the following example:

```
ObjectManager l c jwt <JSON-Web-Token> c:\import data1
```

- Use your Cloud Pak for Data user name and your Cloud Pak for Data API key as in the following example:

```
ObjectManager l c admin <API-Key> c:\import data1
```

An API Key can be generated in Cloud Pak for Data. For more information, see [Generating API keys for authentication](#).

Dump command example

This Windows-based example shows how to export or dump data from IBM OpenPages with Watson to a file with the config1 prefix that resides in the c : \export folder. If the folder does not already exist, the ObjectManager tool creates it. This example uses the Super Administrator account, OpenPagesAdministrator.

Procedure

1. Open a Command Prompt window.
2. Navigate to the bin installation directory, such as:

```
cd C:\OpenPages\bin
```

3. Run the following command on a single line to export data from OpenPages with Watson into the config1-op-config.xml loader file:

```
ObjectManager d c OpenPagesAdministrator OpenPagesAdministrator c:\export config1
```

The file named config1-op-config.xml is created in the c : \export folder.

Batch loader file syntax and sample

A batch loader list file is typically a text (.txt) file that contains a list of the XML loader files for batch processing by the ObjectManager tool.

The ObjectManager tool uses the following syntax for batch loading multiple loader files.

```
ObjectManager <batch-mode> config|c <user> <password> <batch-loader-dir> <batch-loader-list-file>
```

A batch loader list file uses the following rules:

- Any line starting with a pound sign (#) is considered a comment
- Any line starting with greater than sign (>) is written to the screen for display
- All other lines are assumed to be the relative path to a loader file

The following sample batch loader list file was created in a text editor. It shows how to display an informational "loading" message (line starting with >) on the screen for files that are loading from different directories, and provides an example of how to list a loader file (example1-op-config.xml) from a top-level (c : \temp) directory and how to list multiple loader files (example2, example3, example4) from a subfolder (\loaders) located under the top-level directory.

```
# If the <batch-loader-dir> was given as c:\temp, the following lines would
# write the "Loading..." message and then attempt to load the file
# c:\temp\example1-op-config.xml
>Loading example 1...
example1

# If the <batch-loader-dir> was given as c:\temp, the following lines would
# write the "Loading..." message and then attempt to load the files:
# c:\temp\loaders\example2-op-config.xml
# c:\temp\loaders\example3-op-config.xml
# c:\temp\loaders\example4-op-config.xml
>Loading examples 2-4...
loaders\example2
loaders\example3
loaders\example4
```

For example, you save this batch loader list file with the name load-reports.txt in the c : \OpenPages default installation directory.

The instructions in the following example show how to run the sample `load-reports.txt` batch loader list file to load or import data into IBM OpenPages with Watson. The top-level directory (`c:\temp`) is used for the `<batch-loader-dir>` parameter because it includes the loader files in the `\loaders` subfolder.

Procedure

1. Open a Command Prompt window.
2. Navigate to the bin installation directory, such as:

```
cd C:\OpenPages\bin
```

3. Run the following batch command to load the `load-reports.txt` batch loader list file:

```
ObjectManager b c OpenPagesAdministrator password c:\temp load-reports.txt
```

Using ObjectManager to move objects

This example shows how an IBM OpenPages with Watson administrator can move a process object from the folder location `/ENTITY02` to `/ENTITY01`.

Before you begin

This solution assumes that the administrator knows the following:

- The contents of TechNote # 1648075 that explains the difference between system folder location and associations.
- The system-level folder name of the object.
- The target folder location already exists. Otherwise, the following validation will occur:

```
VALIDATION ERROR (Line: 967 Column: 89): Target Folder Resource  
(/_op_sox/Project/Default/ICDocumentation/Processes/SampleFolder001)  
does not exist.
```

About this task

The following is the syntax for moving objects using the ObjectManager tool:

```
<openpagesConfiguration xmlFormatVersion="1.31">  
  <moveResources>  
    <targetFolder name="{fullpath of target folder}">  
      <sourceResource name="{fullpath of the object to be moved}"/>  
    </targetFolder>  
  </moveResources>  
</openpagesConfiguration>
```

Procedure

1. Log onto the application server.
2. Open a text editor.
3. Copy the previous syntax example.
4. Update the example to reflect the target folder location(s) and source folder location(s).

For example:

```
<openpagesConfiguration xmlFormatVersion="1.31">  
  <moveResources>  
    <targetFolder name="/_op_sox/Project/Default/ICDocumentation/  
      Processes/ENTITY01">  
      <sourceResource name="/_op_sox/Project/Default/ICDocumentation/  
        Processes/ENTITY02/PROC01.txt"/>  
    </targetFolder>  
  </moveResources>  
</openpagesConfiguration>
```

5. Save the file using the an ObjectManager name (e.g., `samplemove-op-config.xml`).

6. Open a command prompt or shell. Alternatively, you can use **Administration > Import Configuration** to import the XML file. For information, see [“Importing a migration file \(Standard UI\)”](#) on page 878.
7. Go to *OP_HOME*/bin where *OP_HOME* represents the installation location of the OpenPages with Watson application.
8. Run the command to load the ObjectManager file.

The following is the sample output for the working example:

```
D:\OpenPages\bin>ObjectManager l c
OpenPagesAdministrator OpenPagesAdministrator
D:\temp samplemove

OpenPages V8.1.0.0 (Build: OP_8.1-270 2019/09/06 19:17:21) starting ...
OpenPages Global environment initialized.
=====
Object Manager Admin Utility V8.1.0.0 (Build: OP_8.1-270 2019/09/06 19:27:49)
=====

List of command line arguments:
  Arg 1: <l>
  Arg 2: <c>
  Arg 3: <OpenPagesAdministrator>
  Arg 4: <****>
  Arg 5: <D:\temp>
  Arg 6: <samplemove>
Total number of arguments: 6
OpenPages Server environment initialized.

Loading OpenPages Configuration (samplemove) from folder: 'D:\temp' ...

Processing started at Thu Apr 05 15:51:29 EDT 2013

Processing Move Resource Requests ...
    1 total

Move Resource requests processed: 1

Total Objects processed: 0

Total Requests processed: 1

Total Validation Errors: 0

Total Exceptions: 0

Processing finished at Thu Oct 03 15:51:29 EDT 2019
Elapsed time: 347 milliseconds
```

9. Restart the OpenPages services. For more information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.
10. If an administrator needs to move multiple objects via ObjectManager, the following is the sample syntax:

```
<openpagesConfiguration xmlFormatVersion="1.31">
  <moveResources>
    <targetFolder name="{target fullpath folder for object 1}">
      <sourceResource name="{fullpath of the object 1 to be moved}"/>
    </targetFolder>
    <targetFolder name="{target fullpath folder for object 2}">
      <sourceResource name="{fullpath of the object 2 to be moved}"/>
    </targetFolder>
    <targetFolder name="{target fullpath folder for object 3}">
      <sourceResource name="{fullpath of the object 3 to be moved}"/>
    </targetFolder>
  </moveResources>
</openpagesConfiguration>
```

Using ObjectManager to rename objects

This example shows how an IBM OpenPages with Watson administrator can rename an entity from ENTITY01 to ENTITY01A.

Before you begin

The following solution assumes that the administrator knows the system-level folder name of the object. Otherwise, the following message will be displayed:

```
VALIDATION ERROR (Line: 968 Column: 55): Resource to rename
(/_op_sox/Project/Default/BusinessEntity/ENTITY_oldname/ENTITY_oldname.txt)
does not exist.
```

About this task

The following is the ObjectManager syntax for renaming objects:

```
<openpagesConfiguration xmlFormatVersion="1.31">
  <renameResources>
    <renameResource oldFullName="{fullpath of the object to be renamed}"
      newShortName="{name new of the object}.txt"/>
  </renameResources>
</openpagesConfiguration>
```

Procedure

1. Log onto the application server.
2. Open a text editor.
3. Copy the previous syntax example.
4. Update the example to reflect the target folder location(s) and source folder location(s).

For example:

```
<openpagesConfiguration xmlFormatVersion="1.31">
  <renameResources>
    <renameResource oldFullName="/_op_sox/Project/Default/
      BusinessEntity/ENTITY01/ENTITY01.txt"
      newShortName="ENTITY01A.txt"/>
  </renameResources>
</openpagesConfiguration>
```

5. Save the file using the ObjectManager file name format, such as samplerename-op-config.xml.
6. Open a command prompt or shell. Alternatively, you can use **Administration > Import Configuration** to import the XML file. For information, see [“Importing a migration file \(Standard UI\)” on page 878](#).
7. Go to *OP_HOME*/bin where *OP_HOME* represents the installation location of the OpenPages with Watson application.
8. Run the command to load the ObjectManager file.

The following is the sample output for the working example:

```
D:\OpenPages\bin>ObjectManager l c OpenPagesAdministrator
OpenPagesAdministrator D:\temp samplerename

OpenPages V8.1.0.0 (Build: OP_8.1-270 2019/09/06 19:17:21) starting ...
OpenPages Global environment initialized.
=====
Object Manager Admin Utility V8.1.0.0 (Build: OP_8.1-270 2019/09/06 19:27:49)
=====

List of command line arguments:
Arg 1: <l>
Arg 2: <c>
Arg 3: <OpenPagesAdministrator>
Arg 4: <****>
Arg 5: <D:\temp>
Arg 6: <samplerename>
Total number of arguments: 6
OpenPages Server environment initialized.

Loading OpenPages Configuration (samplerename) from folder: 'D:\temp' ...

Processing started at Fri Apr 05 08:48:21 EDT 2013

Processing Rename Resource Requests ...
  1 total
```

```

Rename Resource requests processed: 1
Total Objects processed: 0
Total Requests processed: 1
Total Validation Errors: 0
Total Exceptions: 0

Processing finished at Fri Oct 04 08:48:23 EDT 2019
Elapsed time: 2418 milliseconds

```

- Restart the OpenPages services. For more information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.

If an administrator needs to rename multiple objects via ObjectManager, the following is the sample syntax:

```

<openpagesConfiguration xmlFormatVersion="1.31">
  <renameResources>
    <renameResource oldFullName="{fullpath of the object 1 to be renamed}"
      newShortName="{name new of the object 1}.txt"/>
    <renameResource oldFullName="{fullpath of the object 2 to be renamed}"
      newShortName="{name new of the object 2}.txt"/>
    <renameResource oldFullName="{fullpath of the object 3 to be renamed}"
      newShortName="{name new of the object 3}.txt"/>
  </renameResources>
</openpagesConfiguration>

```

Using ObjectManager to assign or revoke role assignments

An IBM OpenPages with Watson administrator can assign or revoke role assignments using the ObjectManager tool.

Before you begin

This solution assumes that the administrator knows the following items:

- The system-level folder name of the security domain.
- The role assignment type of the role template.
- The role template name.
- The OpenPages with Watson user name.

About this task

The ObjectManager syntax for revoking or assigning a role assignment is as follows:

```

<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
  <roleAssignments>
    <roleAssignment type="{object type}" status="{assign/revoke}">
      <businessUnits>
        <businessUnit name="{path of the security domain}"/>
      </businessUnits>
      <roleActors>
        <roleActor name="{actorname}"/>
      </roleActors>
      <roles>
        <role name="{role template name}"/>
      </roles>
    </roleAssignment>
  </roleAssignments>
</openpagesConfiguration>

```

Using the following example, an administrator can revoke the user johndoe from the root level security domain.

Procedure

1. Log on to the application server.
2. Open a text editor.
3. Copy the syntax example.
4. Update the example to reflect the correct role assignment type: whether to assign or revoke the role; the security domain path; name of actor; and the role template name. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
  <roleAssignments>
    <roleAssignment type="SOXBusEntity" status="revoke">
      <businessUnits>
        <businessUnit name="/_op_sox/Project/Default/BusinessEntity"/>
      </businessUnits>
      <roleActors>
        <roleActor name="johndoe"/>
      </roleActors>
      <roles>
        <role name="OpenPages Modules 7.0 - All Data - No Admin"/>
      </roles>
    </roleAssignment>
  </roleAssignments>
</openpagesConfiguration>
```

5. Save the file using the ObjectManager file name format, such as groupmem-revoke-op-config.xml.
6. Open a command prompt or shell. Alternatively, you can use **Administration > Import Configuration** to import the XML file. For information, see [“Importing a migration file \(Standard UI\)” on page 878](#).
7. Go to *OP_HOME\bin* folder.
8. Run the command to load the ObjectManager file.

The following extract is the sample output for the working example:

```
OpenPages V8.1.0.0 (Build: OP_8.1-270 2019/09/06 14:20:23)
starting ...
OpenPages Global environment initialized.
=====
Object Manager Admin Utility V8.1.0.0
(Build: OP_8.1.0.0-270 2019/09/06 14:20:23)
=====

List of command line arguments:
  Arg 1: <load>
  Arg 2: <config>
  Arg 3: <OpenPagesAdministrator>
  Arg 4: <****>
  Arg 5: <C:\temp>
  Arg 6: <groupmem-revoke>
Total number of arguments: 6
OpenPages Server environment initialized.

Loading OpenPages Configuration (groupmem-revoke) from folder:
'C:\temp' ...

Processing started at Fri Jun 13 14:00:52 EDT 2014

Loading Role Assignments ...
  1 total

Role Assignments processed: 1
Business Units processed: 1
Role Actors processed: 1
Roles processed: 1

Total Objects processed: 4
Total Validation Errors: 0

Total Exceptions: 0
Processing finished at Fri Jun 13 14:00:58 EDT 2014
Elapsed time: 5703 milliseconds
```

- Restart the OpenPages services. For more information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.

Using ObjectManager to create or load users

This example shows how an IBM OpenPages with Watson administrator can create or load users into the system.

Before you begin

This solution assumes that the OpenPages administrator has already created the groups that are referenced in the example.

About this task

The following is the syntax for creating or loading users by using the ObjectManager tool:

```
<openpagesConfiguration xmlFormatVersion="1.31">
  <actors>
    <actor
      name="{username}"
      type="User"
      password="{password}"
      firstName="{firstname}"
      middleName=""
      lastName="{lastname}"
      canChangePassword="{true/false}"
      isTemporaryPassword="{true/false}"
      passwordExpiresInDays="0"
      description=""
      emailAddress="{email_address}"
      locale="{locale}"
      adminLevel="Default"
      enabled="true"
      hidden="false"
      editable="true">
    </actor>
  </actors>
  <actorGroupMemberships>
    <actorGroupMembership name="{username}" isEntityGroup="false">
      <group name="{existing_group_name}" isEntityGroup="false"/>
      <group name="OpenPages" isEntityGroup="false"/>
    </actorGroupMembership>
  </actorGroupMemberships>
</openpagesConfiguration>
```

Procedure

- Log on to the application server.
- Open a text editor.
- Copy the syntax example that is included earlier in this topic into the text editor.
- Modify the example to reflect the actual users and groups details. For example, you can modify the example in the following way:

```
<openpagesConfiguration xmlFormatVersion="1.31">
  <actors>
    <actor
      name="johndoe"
      type="User"
      password="openpages123"
      firstName="John"
      middleName=""
      lastName="Doe"
      canChangePassword="true"
      isTemporaryPassword="false"
      passwordExpiresInDays="0"
      description=""
      emailAddress="john.doe.user@company.com"
      locale="U.S. English"
      adminLevel="Default"
```

```

        enabled="true"
        hidden="false"
        editable="true">
    </actor>
</actors>
<actorGroupMemberships>
    <actorGroupMembership name="johndoe" isEntityGroup="false">
        <group name="All_Users" isEntityGroup="false"/>
        <group name="OpenPages" isEntityGroup="false"/>
    </actorGroupMembership>
</actorGroupMemberships>
</openpagesConfiguration>

```

5. Save the file using the ObjectManager file name format, such as loadusers-op-config.xml.
6. Open a command prompt or a shell and follow the instructions below. Alternatively, you can use **Administration > Import Configuration** to import the XML file. For information, see [“Importing a migration file \(Standard UI\)”](#) on page 878.
7. Go to *OP_HOME*/bin directory where *OP_HOME* represents the installation location of the OpenPages with Watson application.
8. Run the command to load the ObjectManager file. The following is the sample output for the example:

```

=====
ObjectManager Admin Utility V8.1.0.0
=====
List of command line arguments:
  Arg 1: <l>
  Arg 2: <c>
  Arg 3: <OpenPagesAdministrator>
  Arg 4: <****>
  Arg 5: <C:\temp>
  Arg 6: <loadusers>
Total number of arguments: 6
OpenPages Server environment initialized.

Loading OpenPages Configuration (userz2) from folder: 'C:\temp' ...

Processing started at Mon Oct 23 14:00:00 EST 2019

Loading Actors ...
  1 total

Loading Actor Group Memberships ...
  1 total

Actors processed: 1 (1 updated)
Actor Group Memberships processed: 1

Total Objects processed: 2

Total Validation Errors: 0

Total Exceptions: 0

Processing finished at Mon Feb 23 14:00:59 EST 2015
Elapsed time: 454 milliseconds

C:\OpenPages\bin>

```

9. Restart the OpenPages services. For more information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.

Modifying the ObjectManager properties file

The `ObjectManager.properties` file contains settings that control or limit the scope of exported (dumped) configuration and related data from the ObjectManager tool.

Depending on your export activity, modify the value of configuration or migration settings. Edit the `ObjectManager.properties` file in any text editor.

Note: Before you modify the `ObjectManager.properties` file, make a backup copy of the file.

For a list of settings and descriptions, see [“Settings in the ObjectManager.properties file”](#) on page 893.

To determine the settings in the file require modification, refer to the following topics:

- [“Exporting all currency exchange rates” on page 903](#)
- [“Exporting currency field definitions” on page 905](#)
- [“Exporting computed field definitions” on page 906](#)
- [“Migrating configuration changes using the ObjectManager tool” on page 907](#)

The `ObjectManager.properties` file is located in the `<OP_HOME>/bin` directory of your IBM OpenPages with Watson installation.

Table 268. Installation location of the OpenPages with Watson application	
Operating system	Installation location
Windows	For example, <code><OP_Home> C:\IBM\OpenPages</code>
Linux	For example, <code><OP_Home> /opt/IBM/OpenPages</code>

Settings in the `ObjectManager.properties` file

The `ObjectManager.properties` file contains several settings or properties that you can configure.

The logger property

`object.manager.logger.settings`

Defines the location of the logging properties file relative to the `bin` directory. Do not change this setting.

- In 8.2.0.4 and later:

```
object.manager.logger.settings=./log4j2.properties
```

- In 8.2.0.3 and earlier:

```
object.manager.logger.settings=./ObjectManagerLogging.properties
```

The `configuration.manager.migrate.configuration.objects`

The `configuration.manager.migrate.configuration.objects` property overwrites the following `configuration.manager.dump.*` properties and is the equivalent of setting these properties to `true`:

- `configuration.manager.dump.bundle.types`
- `configuration.manager.dump.file.upload.content.types`
- `configuration.manager.dump.jsp.based.content.types`
- `configuration.manager.dump.admin.objectprofile.views`
- `configuration.manager.dump.form.based.content.types`
- `configuration.manager.dump.object.profiles`
- `configuration.manager.dump.application.string.key.categories`
- `configuration.manager.dump.application.string.keys`
- `configuration.manager.dump.application.strings`
- `configuration.manager.dump.object.strings`
- `configuration.manager.dump.error.strings`
- `configuration.manager.dump.query.definitions`
- `configuration.manager.dump.field.dependency`

- `configuration.manager.dump.field.dependency.picklist`
- `configuration.manager.dump.recursive.hierarchy`
- `configuration.manager.dump.date.dimension.type`
- `configuration.manager.dump.object.type.dimension`
- `configuration.manager.dump.date.dimension.type.associations`
- `configuration.manager.dump.recursive.hierarchy.strings`
- `configuration.manager.dump.date.dimension.type.strings`
- `configuration.manager.dump.object.type.dimension.strings`
- `configuration.manager.dump.content.type.relationship.sets`
- `configuration.manager.dump.actor.object.profile.associations`
- `configuration.manager.dump.locales`
- `configuration.manager.dump.role.templates`
- `configuration.manager.dump.role.administrators`
- `configuration.manager.dump.role.assignments`
- `configuration.manager.dump.subsystem.exclusion.fields`
- `configuration.manager.dump.registry`
- `configuration.manager.dump.process.definitions`
- `configuration.manager.dump.tbrules`
- `configuration.manager.dump.tbcalculations`

Additionally, the `configuration.manager.migrate.configuration.objects` property exports the following data:

- Any object folders referenced by:
 - `jsp.based.content.types`
 - `form.based.content.types`
- query definition (filter) strings
- reporting schema column definitions (which are used to keep framework labels consistent when you have duplicate field names).

The `configuration.manager.dump.*` export properties

The following list describes the behavior of the various export `configuration.manager.dump.*` properties when a property is enabled (the value is set to `true`).

`configuration.manager.dump.modules`

Exports a list of the modules (solutions) that are installed. It also controls the list of entries on the **About OpenPages with Watson** and **Build Information** pages.

`configuration.manager.dump.file.types`

Exports a list of valid file attachment types (such as `docx`, `pdf`, `jpg`).

`configuration.manager.dump.bundle.types`

Exports all field groups in the system, along with all of their fields.

`configuration.manager.dump.file.upload.content.types`

Exports all file upload object types, such as **SOXDocument**. It will also export any folders (`nonFormBasedResources`) that are referenced by these object types.

`configuration.manager.dump.jsp.based.content.types`

Exports all other object types, such as **SOXBusEntity**, **Mandate**, **Policy**, or any “Custom Forms”. It will also export any folders (`nonFormBasedResources`) that are referenced by these object types.

`configuration.manager.dump.content.type.relationship.sets`

Exports a list of which objects types can be associated to what other object types.

configuration.manager.dump.app.permissions

Exports a list of application permissions that can be granted to groups or role templates.

configuration.manager.dump.actors

Exports all users, groups, and security domain groups.

configuration.manager.dump.actor.group.memberships

Exports all group memberships, such as: which users belong to what groups, which users belong to what security domains, and which security domains belong to what other security domains.

configuration.manager.dump.actor.object.profile.associations

Exports users and their assigned profiles.

configuration.manager.dump.admin.objectprofile.views

Exports object profiles. This property should be used with the `configuration.manager.dump.object.profiles` setting.

configuration.manager.dump.object.profiles

Exports object profiles. This property should be used with the `configuration.manager.dump.admin.objectprofile.views` setting.

configuration.manager.dump.non.form.based.resources

Exports all folders and object instances in the system. You can use the setting `configuration.manager.dump.resources.root.folder` to narrow the scope of objects that are exported. You will probably want to use this setting with the setting `configuration.manager.dump.resource.sets`.

As an alternative, you can use the `configuration.manager.dump.associated.resources` property.

configuration.manager.dump.form.based.content.types

Exports form-based object type definitions if these were used. By default (out of the box), the software does not use form-based object type definitions.

configuration.manager.dump.form.based.resources

Exports instances of form-based object types if these were used. This property is similar to the `configuration.manager.dump.non.form.based.content.types` property.

The `configuration.manager.dump.form.based.resources` property is generally not needed because of what is stated in the `configuration.manager.dump.form.based.content.types` property.

configuration.manager.dump.channels

Exports all reports that appear on the **Reporting** menu in the IBM OpenPages with Watson application, such as: all JSP reports and any Cognos reports that have been published to the OpenPages with Watson application. It does not export any report definitions from Cognos. If you want to export JSP report definitions, you will also want to set the `configuration.manager.dump.non.form.based.resources` property to true, and the `configuration.manager.dump.resources.root.folder` property to /Reports.

configuration.manager.dump.resource.sets

Exports object instance relationships. For example, if you had an entity called Entity ABC that had a child process called Process A, you would set the following properties to true:

- `configuration.manager.dump.non.form.based.resources` property to get the definitions of Entity ABC and Process A
- `configuration.manager.dump.resource.sets` property to get the entry that says Process A is a child of Entity ABC.

As an alternative, you can use the `configuration.manager.dump.associated.resources` property.

configuration.manager.dump.associated.resources

Exports objects and their relationships – you can use it instead of `configuration.manager.dump.non.form.based.resources` and `configuration.manager.dump.resource.sets`.

To filter the scope of the export, you can use the following settings:

configuration.manager.dump.associated.resources.set

The value of this setting, `SOX.ProjectDefault`, is a constant, do not change it.

configuration.manager.dump.associated.resources.label

Enter the name of the reporting period from which you want to export data. If you leave this value blank, it will default to the **Current Report Period**.

configuration.manager.dump.associated.resources.root.node.

[number]

You can create multiple entries with this setting if you increment the *[number]* part of the name. Enter the full paths of the objects (one object per entry) that you want to use as the scope for the data export. To find the full path of the object, you may need to look at the object in OpenPages. The default value of `/_op_sox/Project/Default/Default.txt` will export all of the data in the system.

configuration.manager.dump.associated.resources.include.content.type.

[number]

You can create multiple entries with this setting if you increment the *[number]* part of the name. Enter one object type name per entry that you want to include in the export. As the export process navigates the object tree structure in the system, when it encounters an object that is not of a type listed in these entries, it will not export that object or any of its children. In this way you can limit the scope of exported objects. A blank entry value will include all object types.

To filter export results, add entry values to one of the following settings. Adding entry values to both settings is redundant.

```
configuration.manager.dump.associated.resources.include.content.type.  
[number]
```

```
configuration.manager.dump.associated.resources.exclude.content.type.  
[number]
```

configuration.manager.dump.associated.resources.exclude.content.type.

[number]

You can create multiple entries with this setting if you increment the *[number]* part of the name. Enter one object type name per entry that you want to exclude in the export. As the export process navigates the object tree structure in the system, when it encounters an object that is not of a type listed in these entries, it will not export that object or any of its children. In this way you can limit the scope of exported objects. A blank entry value will include all object types.

configuration.manager.dump.rule.sets

Exports all object reset rule sets.

configuration.manager.dump.rule.set.execute.sessions

Exports the history of object reset executions.

configuration.manager.dump.registry

Exports all settings in the system.

To filter the scope of the export, you can use the following settings:

configuration.manager.migrate.configuration.exclude.registry.entry.

[number]

Excludes entries listed in this setting from export.

configuration.manager.dump.registry.root.entry.

[number]

Sets the scope of settings to be exported.

You can create multiple entries with this property by incrementing the *[number]* part of the name.

configuration.manager.dump.recursive.hierarchy

Exports recursive object levels.

configuration.manager.dump.date.dimension.type

Exports date dimension types.

configuration.manager.dump.object.type.dimension

Exports object type dimensions.

configuration.manager.dump.date.dimension.type.associations

Exports date dimension type associations (what date dimension types are enabled for what fields).

configuration.manager.dump.locales

Exports supported locales (languages). No translations are included.

configuration.manager.dump.application.string.key.categories

Exports the application text folders.

configuration.manager.dump.application.string.keys

Exports application text keys – the list of entries on the **Application Text** page – without translations.

configuration.manager.dump.application.strings

Exports translations for application text.

configuration.manager.dump.recursive.hierarchy.strings

Exports translations for recursive object levels.

configuration.manager.dump.date.dimension.type.strings

Exports translations for date dimension types.

configuration.manager.dump.object.type.dimension.strings

Exports translations for object type dimensions.

configuration.manager.dump.error.strings

Exports translations for error messages.

configuration.manager.dump.object.strings

Exports translations for: object type names, field names, field guidance, section names, and enumerated values.

configuration.manager.dump.job.types

Exports jobs from the Scheduler. It does not export workflows or Java classes that are used by the jobs.

configuration.manager.dump.currency.exchange.rates

Exports exchange rates.

configuration.manager.dump.currencies

Exports the list of valid currencies (enabled and disabled).

configuration.manager.dump.query.definitions

Exports public filters.

configuration.manager.dump.user.preferences

Exports **Alert Notification** settings for each user.

configuration.manager.dump.role.templates

Exports role templates.

configuration.manager.dump.role.administrators

Exports which users are assigned as administrators for what security domains.

configuration.manager.dump.role.assignments

Exports which users are assigned which role templates for what security domains.

configuration.manager.dump.field.dependency

Exports field dependencies.

configuration.manager.dump.field.dependency.picklist

Exports dependent picklists.

configuration.manager.dump.subsystem.exclusion.fields

Exports fields that are excluded from the reporting subsystem.

configuration.manager.dump.record.level.security.rulesets

Exports rule sets from record level security.

configuration.manager.dump.process.definitions

Exports GRC workflow definitions.

configuration.manager.dump.dashboard.views

Exports dashboards from the Task Focused UI.

configuration.manager.dump.responsive.views

Exports views from the Task Focused UI.

configuration.manager.dump.tbrules

Exports rules from the **Rules Engine**.

configuration.manager.dump.tbcalculations

Exports calculations from GRC Calculations.

configuration.manager.dump.solutions

Exports solution visualizations from the Task Focused UI.

configuration.manager.dump.themes

Exports themes from the Task Focused UI.

The configuration.manager.force.update.* properties**configuration.manager.force.update.object.strings**

Overwrites existing object strings when set to `true` prior to a load.

The default is `false`. If you change this setting to `true`, the load overwrites existing customized strings. Change it immediately back to `false` after the load is done to protect against inadvertently overwriting customized strings.

configuration.manager.force.update.application.strings

Overwrites existing application strings when set to `true` prior to a load.

The default is `false`. If you change this setting to `true`, the load overwrites existing customized strings. Change it immediately back to `false` after the load is done to protect against inadvertently overwriting customized strings.

The invalid characters property**configuration.manager.property.name.illegal.characters=!@#%&*()<>+=[\|/}{ }?**

Defines characters that cannot be used in field names.

The disable triggers properties**configuration.manager.migrate.configuration.disable.all.triggers=/OpenPages/Applications/GRCM/Disable Triggers**

Points to the registry setting that indicates whether triggers are disabled or not. Do not change it. It works with the `configuration.manager.disable.triggers` setting.

configuration.manager.disable.triggers

Disables triggers when importing or exporting data in order to not trigger excess processing as objects are created, modified, or associated. If set to `true`, triggers are disabled at the start of the import or export and re-enabled at the end. Default is `false`.

The resource load property**configuration.manager.load.resource.ignore.undefined.property.value**

Controls behavior when loading objects. For more information, see [“Controlling data load behavior”](#) on page 901.

Filtering data for export

By using a filters file with predefined filters, you can narrow the scope of configuration and related data that is exported from the IBM OpenPages with Watson repository by the ObjectManager tool.

Before you begin

Before you can export selected data using a filters configuration file, you must verify that all dump configuration settings in the `ObjectManager.properties` file are correctly set.

Any settings in the `ObjectManager.properties` file that start with the following code must have its value set to `true`. If the value is set to `false`, then change the value to `true`.

```
configuration.manager.dump.<property>=true
```

For example, `configuration.manager.dump.object.profiles=true`

For details on modifying the `ObjectManager.properties` file, see [“Modifying the ObjectManager properties file”](#) on page 892.

About the filters configuration file

Filters are defined in an XML-based configuration file that must be named `ObjectManagerExportFilters.xml` and must be stored in the `<OP_HOME>` directory:

```
<OP_HOME>/ObjectManagerExportFilters.xml
```

The XML tags used for specifying the predefined filters are the same as the ObjectManager configuration loader XML tags. Most filters are defined on the name attribute of an object. Some filters have either additional or different filter attributes.

For a list of predefined filters, see [Table 269](#) on page 899.

You can use the following sample file: `<OP_HOME>/bin/ObjectManagerExportFilters-Example.xml`. Make a copy of the file, change the file name to `ObjectManagerExportFilters.xml`, make your changes, and copy the file to `<OP_HOME>`.

Example

The following sample filter code shows how you can use the ObjectManager tool to export only the object profile with the name `Default`. No other object types or any other profiles will be exported.

```
<objectProfiles>
  <!-- List of names of profiles to export -->
  <objectProfile name="Default"/>
</objectProfiles>
```

After defining the filters in the filters configuration file, you can use the ObjectManager dump command to export the objects.

ObjectManager predefined filters

The following predefined filters are supported in the ObjectManager tool.

[Table 269](#) on page 899 lists the various element types with their corresponding element tag and filter attributes.

Table 269. ObjectManager predefined filters			
Element type	Element tag	Filter attribute	Comment
Application Text	<application String>	name	The name of the application string.

Table 269. ObjectManager predefined filters (continued)

Element type	Element tag	Filter attribute	Comment
Channels	<channel>	Any of the following: • name • channelFolder (name) • pageTemplate (name)	The name of the reporting folder or path of the reporting folder or page template.
Currencies	<currency>	isoCode	The 3-letter ISO currency code.
Exchange Rates	<exchangeRate>	isoCode	The 3-letter ISO currency code.
Field Groups	<bundleType>	name	The name of the field group.
File based resources	<resource>	name	The full path of the resource.
Filters	<queryDefinition>	name	The name of the Query definition.
Job Types	<jobType>	name + (the associated bundles)	The name of the job type.
Object Profiles	<objectProfile>	name	The name of the object profile.
Object Profile Views	<objectProfileView>	Any of the following: • type • name	Either the type only or the type and name of the Activity view.
Object Reset (SCOR) Rulesets	<ruleSet>	name	The name of the set.
Object Types	<contentType>	name	The name of the object type.
Object Type Pick List Dependencies	<dependencySet>	objectType	The object for which dependencies are defined.
Object Type Relationships	<contentType Relationship>	Any of the following: • parent • child	The parent and/or child object types.
Object Text	Any of the following: • <objectTypeString> • <fieldString> • <enumValueString> • <viewString> • <sectionString>	name	The data for the selected string.

Table 269. ObjectManager predefined filters (continued)

Element type	Element tag	Filter attribute	Comment
Role Templates	<roleTemplate>	name	The name of the Role Template.
Settings	<registryEntry>	name	The name of the setting.
Sub-system Field Extensions	<subSystemExclusion ObjectType>	name	The name of the excluded object type.
User Group Memberships	<actorGroup Membership>	name	For all groups.
	<group>	name	For all group members.
Workflow definitions	<processDefinition>	- name - objectType	
Rules (in the Rules Engine)	<tbRule>	- name - objectType	

Sample filter configuration file

The following sample ObjectManagerExportFilters.xml filter file exports configuration data for only the Object Profile named Default and its associated Detail and Activity Views.

```
<openpagesConfigurationFilters xmlFormatVersion="1.0">
  <objectProfiles>
    <!-- List of names of profiles to export -->
    <objectProfile name="Default"/>
  </objectProfiles>

  <objectProfileViewsSet>
    <!-- Specifiy the name of the profile -->
    <objectProfileViews name="Default">
      <!-- Specifiy the name of the object type in the profile -->
      <objectProfileViewsForObjectType name="SOXProcess">
        <!-- Specifiy the views and their names -->
        <objectProfileView type="Detail"/>
        <objectProfileView type="Activity" name="Process AV"/>
      </objectProfileViewsForObjectType>
    </objectProfileViews>
  </objectProfileViewsSet>
</openpagesConfigurationFilters>
```

Controlling data load behavior

To control the behavior of the ObjectManager tool when loading objects, you can modify a setting in the ObjectManager.properties file.

By setting the configuration.manager.load.resource.ignore.undefined.property.value in the ObjectManager.properties file, you can control whether the ObjectManager tool creates objects with undefined values (such as an empty value or a value without a default). This setting applies only to non-required fields.

Note: If a field is required and has no default value defined, then the ObjectManager tool:

- Ignores the setting in the configuration.manager.load.resource.ignore.undefined.property.value property

- Does not create the object instance
- Reports validation errors.

Procedure

1. Open the `ObjectManager.properties` file in a text editor of your choice (see [“Modifying the ObjectManager properties file”](#) on page 892).
2. Set the value of the `configuration.manager.load.resource.ignore.undefined.property.value` property. If you set the value to:
 - `true` - then ObjectManager creates the object without validation errors. This value is the default.
 - `false` - then ObjectManager reports validation errors, does not create the object, and moves to the next object in the loader file.
3. Run the ObjectManager tool (see [“Running ObjectManager commands”](#) on page 882).

Managing currency exchange rates

You can use XML elements in ObjectManager loader files to update, export, and enable or disable currency exchange rates.

Note: To use these functions, the currency must have a standard 3-letter ISO code and exist in your system.

There are several methods for updating currency exchange rates:

- Use the **Currencies** task in the Task Focused UI. For more information, see [“Editing, enabling, disabling, and uploading currency exchange rates \(Task Focused UI\)”](#) on page 215.
- The **Administration > Currencies** task in the Standard UI. For more information, see [“Uploading a CSV file \(Standard UI\)”](#) on page 237 and [“Editing exchange rates for an existing currency code \(Standard UI\)”](#) on page 237.
- An ObjectManager loader file. For more information, see [“Importing exchange rates”](#) on page 902.

Importing exchange rates

Use a data loader file to import exchange rates for existing currency codes by specifying the new rates in the file or by uploading a properly formatted CSV file with the new rates.

Note: For CSV file format information, see [“Formatting a CSV file”](#) on page 214.

Before you begin

To use this function, the currency must have a standard three letter ISO code and exist in your system.

Procedure

1. Create an XML data loader file (see [“Creating a data loader file”](#) on page 882).
2. To load exchange rate data:
 - If the exchange rate data is specified in a loader file - use the element tags in the following example and substitute the values of the attributes that are listed in the table:

Table 270. Element tags		
Element	Attribute	Description
exchangeRate	isoCode	A three letter ISO currency code
exchangeRate	rate	The currency exchange rate

The following example loads currency exchange rates for the Canadian dollar (CAD) and Mexican peso (MXN).

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
  <exchangeRates>
    <exchangeRate isoCode="CAD"
      startDate="2018-05-09 17:36:12"
      rate="0.8636"/>
    <exchangeRate isoCode="MXN"
      startDate="2018-05-09 17:36:12"
      rate="0.0951"/>
  </exchangeRates>
</openpagesConfiguration>
```

- If the exchange rate data is contained in a CSV file for upload, use the element tag in the following example to upload a .csv file. Substitute the value of the attribute that is listed in the table:

Table 271. Element tag to upload a .csv file

Element	Attribute	Description
uploadFile	name	The file path and name of the CSV file

For example:

```
<uploadFile name="c:\loaders\rate-update1.csv" dataType="Exchange Rates" />
```

3. Use the ObjectManager load command to import the data. See the [“Load command example”](#) on page 884.

Exporting all currency exchange rates

To export (dump) all the currency exchange rates from your system, you must modify some of the settings in the ObjectManager.properties file.

For information about the file, see [“Modifying the ObjectManager properties file”](#) on page 892.

Before you begin

To use this function, the currency must have a standard 3-letter ISO code and exist in your system.

Procedure

1. In the ObjectManager.properties file:

- a) Set the values of the following properties as shown:

```
configuration.manager.migrate.configuration.objects=false
```

```
configuration.manager.dump.currency.exchange.rates=true
```

- a) Set the dump options for all other objects to false.

2. Use the ObjectManager dump command to export the data. See the [“Dump command example”](#) on page 885.

Enabling and disabling currencies

You can enable one or more currencies to make it available to the appropriate processes, or you can disable one or more currencies from IBM OpenPages with Watson.

A disabled currency can be enabled later.

Before you begin

To use this function, the currency must have a standard three letter ISO code and exist in your system.

Procedure

1. Create an XML data loader file (see [“Creating a data loader file”](#) on page 882).
2. To enable or disable one or more currencies, use the element tags in the following example and substitute the values of the attributes that are listed in the table:

Table 272. Elements to enable or disable currencies		
Element	Attribute	Description
currency	isoCode	A three letter ISO currency code
currency	enabled	If you set the value to: • true - the currency is enabled • false - the currency is disabled

The following example enables Euros and disables United Kingdom pounds.

```
<currencies>
  <currency isoCode="EUR"
    enabled="true"/>
  <currency isoCode="GBP"
    enabled="false"/>
</currencies>
```

3. Use the ObjectManager load command to import the data. See the [“Load command example”](#) on page 884.

Importing currency field definitions

You can import currency field definitions.

Before you begin

In IBM Db2 environments, before you import an ObjectManager load that contains metadata definitions (such as fields, field groups, object type, object type associations), drop the reporting schema. Then, when the import completes, recreate the reporting schema.

Procedure

1. Create an XML data loader file (see [“Creating a data loader file”](#) on page 882).
2. To import currency field definitions, use the element tags in the following example and substitute the values of the attributes listed in the table:

Table 273. Elements for importing currency field definitions		
Element	Attribute	Description
bundleType	name	The name of a field group
bundleType	description	A brief description of the field group
propertyType	name	The name of a currency field within the specified field group
propertyType	description	A brief description of the currency field
propertyType	required	If you set the element to one of the following values: • true - the field is required • false - the field is not required

Table 273. Elements for importing currently field definitions (continued)		
Element	Attribute	Description
propertyType	multiValued	If you set the element to one of the following values:: • true - multiple values can be selected from the list • false - only one value can be selected from the list

The following example loads the definition for the currency field "testCurrency" that belongs to a group of the same name.

```
<bundleTypes>
  <bundleType name="testCurrency"
    description="Sarbanes-Oxley Self-Assessment system bundle"
    type="Content Type">
    <propertyType name="testCurrency"
      description="Annualized Value may be used to capture the account
balance from operational systems."
      dataType="Currency"
      minValue=""
      maxValue=""
      defaulttValue=""
      required="false"
      currencyCode=""
      multiValued="false">
    </propertyType>
  </bundleType>
</bundleTypes>
```

3. Use the ObjectManager load command to import the data. See the [“Load command example”](#) on page 884.

Exporting currency field definitions

To export (dump) currency field definitions from your system, you must modify some of the settings in the ObjectManager.properties file.

For information about the file, see [“Modifying the ObjectManager properties file”](#) on page 892.

Procedure

1. In the ObjectManager.properties file, set the values of the following properties as shown:

```
configuration.manager.migrate.configuration.objects=false
configuration.manager.dump.bundle.types=true
```

Tip: When you use ObjectManager to export all object instances and their relationships, and you have a large dataset, ObjectManager will report an exception in ObjectManager.log. To avoid the exception, limit the size of the data that is exported by specifying a folder path or selecting the specific objects in the hierarchy. To specify a folder path, add the following property: configuration.manager.dump.resources.root.folder=folder_path. To specify multiple objects whose hierarchies are to be exported, add the following property, where number is a positive integer:

```
configuration.manager.dump.associated.resources.root.node.n=number
```

2. Use the ObjectManager dump command to export the data. See the [“Dump command example”](#) on page 885.

Importing computed field definitions

You can import computed field definitions.

For information on computed fields, see [“Defining a computed field”](#) on page 227.

Before you begin

In IBM Db2 environments, before you import an ObjectManager load that contains metadata definitions (such as fields, field groups, object type, object type associations), drop the reporting schema. Then, when the import completes, re-create the reporting schema.

Procedure

1. Create an XML data loader file (see [“Creating a data loader file”](#) on page 882).
2. To import computed field definitions, use the element tags in the following example and substitute the values of the attributes listed in the table:

Table 274. Elements to import computed field definitions		
Element	Attribute	Description
computationHandler	name	Do not change. A field definition attribute of the computed field.
computationHandler	value	A value that corresponds to a particular field definition attribute.

The following example loads the definition of a computed field.

```
<computationHandler name="CognosComputationHandler">
  <computationHandlerAttribute name="Equation"
    value="count(distinct
[DEFAULT].[SOXTEST].[TE_TEST_ID])"/>
  <computationHandlerAttribute name="Namespace"
    value="DEFAULT"/>
  <computationHandlerAttribute name="Object ID Column"
    value="Just some text"/>
  <computationHandlerAttribute name="Reporting Period ID
Column"
    value="Value for testing"/>
</computationHandler>
```

3. Use the ObjectManager load command to import the data. See the [“Load command example”](#) on page 884.

Exporting computed field definitions

To export (dump) computed field definitions from your system, you must modify some of the settings in the ObjectManager.properties file.

For information about the file, see [“Modifying the ObjectManager properties file”](#) on page 892.

Procedure

1. In the ObjectManager.properties file, set the value of the following property as shown:
configuration.manager.migrate.configuration.objects=true

Tip: When you use ObjectManager to export all object instances and their relationships, and you have a large dataset, ObjectManager will report an exception in ObjectManager.log. To avoid the exception, limit the size of the data that is exported by specifying a folder path or selecting the specific objects in the hierarchy. To specify a folder path, add the following property: configuration.manager.dump.resources.root.folder=*folder_path*. To specify multiple objects whose hierarchies are to be exported, add the following property: configuration.manager.dump.associated.resources.root.node.n=*number*, where *number* is a positive integer.

2. Set the dump options for all other objects to false.
3. Use the ObjectManager dump command to export the data. See the [“Dump command example”](#) on page 885.

Exporting file attachments

This example shows how an IBM OpenPages with Watson administrator can export file attachments.

Procedure

1. Log on to the application server.
2. Edit the `ObjectManager.properties` file. Configure all properties to be false except for the following property:

```
configuration.manager.dump.non.form.based.resources=true
```

If you want to limit the export to a specific system folder and its subfolders, set the `configuration.manager.dump.resources.root.folder` property.

For example:

```
configuration.manager.dump.resources.root.folder=/_op_sox_documents/Files and Forms/  
Company ABC/SubEntity Folder
```

3. Save the file.
4. Open a command prompt or a shell.
5. Go to the `OP_HOME/bin` directory where `OP_HOME` represents the installation location of the OpenPages with Watson application.
6. Run the following command:

```
ObjectManager.cmd|sh d c <user> <password> <file_location> <file_name_prefix>
```

For example, the following syntax creates a file called `ExportedFile-op-file-content.zip` in the `C:\TMP` directory.

```
ObjectManager d c OpenPagesAdministrator password C:\TMP ExportedFile
```

Migrating configuration changes using the ObjectManager tool

You can use the ObjectManager tool to migrate configuration changes from one deployment environment to another.

The source and target environments must have the same version and patch level of OpenPages with Watson.

Multi-deployment environments

If you have a multi-deployment environment where changes to the IBM OpenPages with Watson application are tested and validated prior to implementation, you can use ObjectManager, a command line interface (CLI) tool, to migrate configuration changes from one deployment environment to another.

Multi-deployment environments may vary from company to company. For example, a multi-deployment environment for "Company 1" might contain the following deployments:

- Development Deployment - configuration changes are made to the user interface and tested to validate that the changes are applied correctly. The OpenPages with Watson repository used in this deployment might contain fewer objects (partial instance data) than the Production deployment.
- Test Deployment - configuration changes from the Development configuration are imported (to avoid error) and validated through the ObjectManager tool and tested. The OpenPages with Watson repository used in this deployment generally mirrors the instance data in the Production deployment.
- Production Deployment - The tested configuration changes from the Test configuration are imported (to avoid error) and validated through the ObjectManager tool, and then made available to end users (Live Production).

"Company 2" might, for example, combine Development and Test into a single Test deployment before migrating configuration changes to a Production environment.

The ObjectManager migration process

Using the ObjectManager tool, you can migrate configuration changes from one deployment to another for the following objects:

- Field Groups
- Object Types
- Filters
- Field Dependencies
- Dependent Picklists
- Object Type Relationships
- Profiles
- Application Text
- Object Text
- Settings (excludes machine-specific settings in the IBM OpenPages with Watson repository)
- Rules (from the **Rules Engine**)
- Workflow definitions in GRC Workflow
- Jobs in the Scheduler
- Calculations (from GRC Calculations)
- Solution visualizations

You can also export and import security rules. However, any existing security rules are overwritten by the import. If you want to migrate security rules, export the security rules from the target environment, modify the exported file to add or modify the security rules, and then import the updated file into the target environment.

To limit the scope of the changes to the previously mentioned configuration objects, you can edit settings in the `ObjectManager.properties` file. For more information, see [“Modifying ObjectManager settings” on page 909](#).

[Table 275 on page 908](#) outlines the process that you can follow if you want to migrate configuration changes, for example, from a Test environment to a Production environment.

Note: If you have a multi-deployment environment that also includes a Development environment, you can use the tasks that are outlined in [Table 275 on page 908](#) to do an initial export of the configuration data from the Development environment to the Test environment.

Table 275. Tasks for migrating configuration changes		
Use this deployment...	To do this task...	Related topic...
Test	1. Modify settings in the <code>ObjectManager.properties</code> file to limit the scope of the export data to only configuration objects.	See “Modifying ObjectManager settings” on page 909 for step-by-step setup instructions before you export configuration data.
Test	2. Export the configuration changes into a file.	See “Exporting configuration changes” on page 911 for step-by-step instructions on how to export configuration metadata.
Production	3. Compare the configuration changes from the previous deployment (in task 2) against this deployment.	See “Validating configuration changes” on page 911 for step-by-step instructions on how to validate configuration changes.

Table 275. Tasks for migrating configuration changes (continued)

Use this deployment...	To do this task...	Related topic...
Production	4. Import the configuration changes (from task 3) into the current deployment.	See “Importing configuration changes” on page 913 for step-by-step instructions on how to update configuration changes.
Production	5. To validate that all the updates were applied, compare the configuration changes from the previous deployment (in task 2) against the newly updated deployment.	See “Validating configuration changes” on page 911 for step-by-step instructions on how to validate configuration changes.

Modifying ObjectManager settings

Before you begin migrating configuration object changes from one deployment to another, you can use the ObjectManager tool to include only configuration objects in the migration process and exclude additional object data, such as Resource or Job Type data, from the migration metadata and changes.

Limiting the export of changes to configuration objects

By default, the ability to export metadata changes is set to include all objects. So that you can export changes made only to configuration objects, you must modify some of the settings in the ObjectManager.properties file.

Procedure

1. In a text editor of your choice, open the ObjectManager.properties file (see [“Modifying the ObjectManager properties file” on page 892](#)).
2. Navigate to the following setting in the file:
`configuration.manager.migrate.configuration.objects=false`
3. Change the value of this setting from false (default) to true (export only configuration object changes) as follows:
`configuration.manager.migrate.configuration.objects=true`
4. When finished, save your changes to the file.
5. If you want to modify IBM OpenPages with Watson repository settings that are excluded, by default, from the migration process, follow the instructions in [“Modifying excluded settings from export” on page 909](#).

Modifying excluded settings from export

If the value of some IBM OpenPages with Watson repository settings were changed to reflect a particular deployment environment, you can optionally exclude these settings from migrating to the next deployment environment.

For example, if the address of the Notification Mail Server differs from the Development machine to the Test machine, you can exclude this setting from the export of configuration metadata and changes.

You can optionally exclude settings from export by modifying the ObjectManager.properties file. A statement that excludes a setting from export has the following syntax:

```
configuration.manager.migrate.configuration.exclude.registry.entry.<n>=<setting>
```

Where:

- <n> is a sequential number.

- `<setting>` is the full path and name of the setting you want to exclude.

By default, OpenPages with Watson excludes certain configuration settings from the export process. These settings are listed in the `ObjectManager.properties` file along with their full path and name. For example:

```
configuration.manager.migrate.configuration.exclude.registry.entry.1=/OpenPages/
Applications/Common/Email/Mail Server
```

You can add additional settings to the list for exclusion or remove an existing setting from the list to include it in the export.

Procedure

1. Open the `ObjectManager.properties` file (see [“Modifying the ObjectManager properties file”](#) on page 892).
2. Locate the following setting in the file - you will use this setting as the basis for creating additional settings for exclusion:

```
configuration.manager.migrate.configuration.exclude.registry.entry.
1=/OpenPages/Applications/Common/Email/Mail Server
```

3. To exclude additional settings from export, copy the line of code in Step 2 and do the following:
 - a) Paste the code at the end of the list (for example, after 21).
 - b) Increment the number (for example, 22).
 - c) Specify a full setting path and name.

For example (do not wrap - use a single line):

```
configuration.manager.migrate.configuration.exclude.registry.entry.
22=/OpenPages/Platform/Reporting Schema/Object URL Generator/Populate Past Periods
```

4. To export a configuration setting that is on the excluded list, remove the line of code for that setting from the list.
5. When finished, save your changes to the properties file.
6. Use the `ObjectManager dump` command to export the data. See [“Dump command example”](#) on page 885. Not all items in the exclude list will be in the XML dump file.

Note: Make changes to the exclusion list by editing the `ObjectManager.properties` file in `ObjectManager`. Changes to `ObjectManager.properties` are ignored if you use Environment Migration.

Disabling triggers when migrating environments

When extracting and restoring environments using `ObjectManager`, you might need to disable any triggers that are checking data validity. This setting is normally applied automatically, but you can disable triggers if the need arises. This procedure disables all triggers in the system.

Procedure

1. Access the **Settings** page (see [Chapter 19, “Viewing the Configuration and Settings page,”](#) on page 597).
2. Expand the **Applications > GRCM** folder hierarchy.
3. Click the **Disable Triggers** setting to open its detail page.
4. In the **Value** field, type `true`.
5. Click **Save**.

Migrating configuration changes

After you modify settings in the `ObjectManager.properties` file, you can begin the migration process.

Migrating configuration changes from one environment to another involves [exporting](#), [validating](#), and [importing](#) the changes.

Note: The source and target environments must have the same version and patch level of OpenPages with Watson.

Exporting configuration changes

Exported data represents a snapshot of the configuration objects in the IBM OpenPages with Watson repository for a particular deployment.

When you export configuration changes, you specify a file path and prefix for the file name in the command line. When the data is exported, the ObjectManager tool automatically appends `-op-config.xml` to the file name prefix to complete the file name.

For example, if you specify the `myconfig` prefix in the command line for the file name, it results in this file name: `myconfig-op-config.xml`.

Procedure

1. Verify that the OpenPages with Watson application is running.
2. Open a command or shell window and change to the `<OP_HOME>/bin` directory of your OpenPages with Watson installation.
3. From the command or shell window, run an ObjectManager command on a single line.
 - a) On a computer running a Microsoft Windows operating system:

```
ObjectManager dump config <admin-user> <password> <config-folder-path> <prefix>
```

- b) On a computer running a Linux operating system:

```
./ObjectManager.sh dump config <admin-user> <password> <config-folder-path> <prefix>
```

Where:

- `<admin-user>` is the user name of the Super Administrator account (for example, `OpenPagesAdministrator`).
- `<password>` is the password of the Super Administrator account.
- `<config-folder-path>` is the file path to the folder where the exported file will reside. If the folder does not already exist, ObjectManager will create it.
- `<prefix>` is the prefix for the file name that will be used by ObjectManager.

For example, on a Windows operating system:

```
ObjectManager dump config OpenPagesAdministrator password c:\temp myconfig
```

4. To compare the exported configuration data against the configuration data in the OpenPages with Watson repository of the next deployment environment, see [“Validating configuration changes” on page 911](#).

Validating configuration changes

After you export or import configuration changes, you can compare the exported data file from the previous deployment environment against the data in the IBM OpenPages with Watson repository of the current deployment environment.

When you run the `validate` command by using the ObjectManager tool:

- The results are displayed on the screen during the validation process. If you want to review the results at a later time, you can re-direct the screen output to a file.
- An `ObjectManager.log` file that contains exception errors is created. This log file is located in the `<config-folder-path>` directory.

Procedure

1. Copy the exported configuration file from the previous deployment environment (for example, Development) to a folder in the current deployment environment (for example, Production).
2. From the `<OP_HOME>/bin` directory of your OpenPages with Watson installation, open a command or shell window.
3. From the command or shell window, run an ObjectManager command on a single line (optionally re-direct the output to a file):
 - a) On a computer running a Microsoft Windows operating system:

```
ObjectManager validate config <admin-user> <password> <config-folder-path> <prefix>
```

- b) On a computer running a Linux operating system:

```
./ObjectManager.sh validate config <admin-user> <password> <config-folder-path> <prefix>
```

Where:

- `<admin-user>` is the user name of the Super Administrator account (for example, OpenPagesAdministrator).
- `<password>` is the password of the Super Administrator account.
- `<config-folder-path>` is the file path to the folder where the exported file will reside. If the folder does not already exist, ObjectManager will create it.
- `<prefix>` is the prefix for the file name that will be used by ObjectManager.

On a Windows operating system, the command in the following example compares configuration data in the export file `myconfig-op-config.xml` located in the `c:\temp` folder to configuration data in the current deployment, and redirects the display output (from a Windows server) to a text file called `config_log.txt` also located in the `c:\temp` folder:

```
ObjectManager validate config OpenPagesAdministrator password c:\temp myconfig
>c:\temp\config_log.txt
```

4. Review the output for any errors.
5. To import the configuration changes and update the repository of the current deployment environment with these changes, see [“Importing configuration changes”](#) on page 913.
6. To validate that the updated repository of the current deployment matches the configuration changes from the export file, repeat Steps 2-4.

Results

Validation errors indicate a problem with the data itself and should be corrected before importing the configuration changes into the next deployment. The following sample validation error shows the name field in the export file as having an empty value.

VALIDATION ERROR (Line: 104481 Column: 57): Attribute 'name' is either empty or not provided.

Verification errors indicate differences in the content of the configuration data between the export file and the OpenPages with Watson repository. The following sample verification error shows a discrepancy in the display label text for the Control Method object field between the export file of the previous deployment (Control Method) and the OpenPages with Watson repository of the current deployment (Implementation Method).

VERIFICATION ERROR (Line: 104873 Column: 52): Attribute 'singularValue' for element 'fieldString'(Control Method) did not verify. XML Value: <Control Method> OPX Platform Value: <Implementation Method>.

When the processing is complete, a summary of the configuration objects that were processed is displayed.

After the repository is updated with the configuration changes from the export file and the validation process is repeated, the data in the export file and in the repository should match and no errors should be displayed.

Importing configuration changes

After comparing and validating the configuration metadata and changes, you can migrate the changes to the current deployment environment or system.

When you import the configuration changes from the previous deployment, the configuration objects in the IBM OpenPages with Watson repository of the current deployment are updated with those changes.

Note: The source and target environments must have the same version and patch level of OpenPages with Watson.

An alternative to using the command line interface (CLI) tool in ObjectManager is to use **Administration > Import Configuration** to import the XML file. For information, see [“Importing a migration file \(Standard UI\)”](#) on page 878.

Procedure

1. Verify that the OpenPages with Watson application is running.
2. Open a command or shell window and change to the `<OP_HOME>/bin` directory of your OpenPages with Watson installation.
3. From the command or shell window, run an ObjectManager command on a single line:
 - a) On a computer running a Microsoft Windows operating system:

```
ObjectManager load config <admin-user> <password> <config-folder-path> <prefix>
```

- b) On a computer running a Linux operating system:

```
./ObjectManager.sh load config <admin-user> <password> <config-folder-path> <prefix>
```

Where:

- `<admin-user>` is the user name of the Super Administrator account (for example, OpenPagesAdministrator).
- `<password>` is the password of the Super Administrator account.
- `<config-folder-path>` is the file path to the folder where the exported file will reside. If the folder does not already exist, ObjectManager will create it.
- `<prefix>` is the prefix for the file name that will be used by ObjectManager.

For example, on a Windows operating system:

```
ObjectManager load config OpenPagesAdministrator password c:\temp myconfig
```

4. To see the configuration changes in the application, stop and then restart the OpenPages with Watson application services.
5. To validate that the newly updated OpenPages with Watson repository matches the configuration changes from the export file, see the topic [“Validating configuration changes”](#) on page 911.
6. To export the configuration data to a file, see the topic [“Exporting configuration changes”](#) on page 911.

What to do next

If you loaded profiles, update the reporting schema. For more information, see [“Updating the reporting schema” on page 162](#).

Chapter 28. Using FastMap

FastMap is a productivity tool that works with the IBM OpenPages with Watson export feature, and automates the importing and batch processing of object data into OpenPages with Watson.

The FastMap tool uses a data load template (a Microsoft Excel workbook in .xls or .xlsx format) to capture data for import. When you import data into OpenPages with Watson, FastMap validates the data and, if no errors are found, populates the repository with the new or updated records.

Sample scenario

You have 150 Process and 175 Risk objects (records) that require either creation or updating. Rather than manually creating or updating individual Process and Risk objects through the OpenPages with Watson application interface, you use a FastMap data load template to capture the data for batch processing.

After the data is captured, log on to the OpenPages with Watson application and import the template (in .xls or .xlsx format) through FastMap for validation. During the validation phase, you receive a few validation errors. You fix the errors in the template and resubmit it. This time, no validation errors are reported and the data is automatically processed. After processing is complete, the objects become available for reports and updating by users.



Attention: When you import an object using FastMap, the imported object settings are usually determined by the **Detail** view settings within the profile.

For example, you are using the Default profile and you want to import SOXControl objects. If the **Detail** view for SOXControl has the **Description** field set to **Read-only**, you cannot update the **Description** field after importing the object via FastMap. In addition, administrators should be aware that field dependency rules are not evaluated for FastMap loads. This allows FastMap users to stage data, requiring users to enter required data during subsequent updates.

This video demonstrates how to use FastMap to import data:

<https://youtu.be/iv9cK3yqtxc>

FastMap overview

This topic provides an overview of the tasks using FastMap to import data into IBM OpenPages with Watson.

Note: FastMap import is not supported for File and Signature objects or for the system Comment field.

The FastMap tool validates and imports object data.

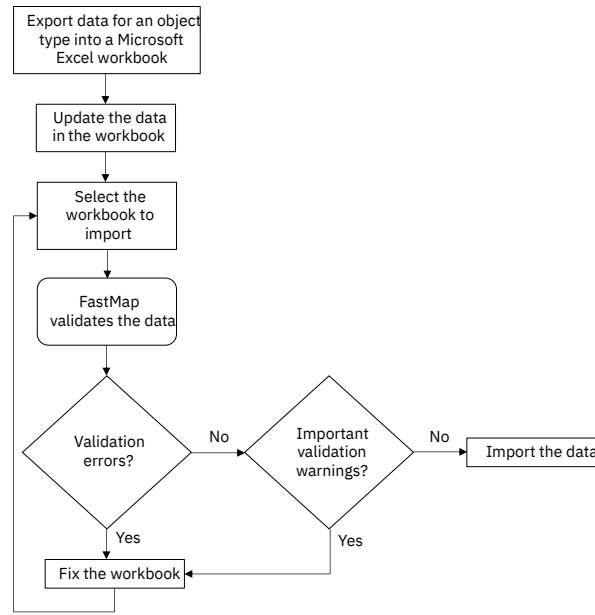


Figure 67. FastMap task flow

The FastMap import process

The following steps provide an overview of the process for creating and using a FastMap template to import data.

Procedure

1. To create a Microsoft Excel workbook, select the items you want to modify and export them.
 - In the Task Focused UI, open a grid view. You can use a filter to show only the items you want to export. Click .
 - To export specific items in the grid view, select the checkboxes to the left of each item that you want to export. A different toolbar is displayed. In the toolbar, click .
 - In the Standard UI, open a Filtered List View. You can use a filter to show only the items you want to export. Click the **Export** icon.
2. In the **Export** dialog box, select any descendant object types you want to export. Click **Export**.
3. Add or modify the object data on the worksheet as needed. Unhide columns if necessary.
4. Optional: Add or modify parameters on the Definition worksheet as needed.

For more information, see [“Using the FastMap Definition worksheet” on page 934](#).
5. Save the file.
6. Import the workbook by choosing one of the following options:
 - In the Task Focused UI, see [“Accessing FastMap to import data and view status \(Task Focused UI\)” on page 918](#).
 - In the Standard UI, see [“Accessing FastMap to import data and view status \(Standard UI\)” on page 919](#).

FastMap templates

A FastMap template is a Microsoft Excel workbook with data load worksheets that you can modify.

A workbook for FastMap import has the following characteristics:

- Contains one or more data load worksheets (must be in .xls or .xlsx format).
- Has only one data load worksheet per object type.
- By default, is in the user's locale.
- Optionally, includes a Definition worksheet in a workbook to configure FastMap import and export behavior.

A data load worksheet within a workbook has the following characteristics:

- Is specific to an object type.
- Has a variety of columns where you specify parent and folder paths and change data for listed objects.
- Each column must have a heading name.
- Optionally, includes one or more special column headings.
- Must contain localized column names and data.

Example

You want only users who are assigned the "Upload Data" profile to import changed or new data for the following five object types: Business Entities, Processes, Risks, Controls, and External Losses. You could either create a workbook with multiple worksheets—one for each object type for a total of five data load worksheets, or multiple workbooks—one for each object type.

Note:

- You cannot import attachments or signatures with FastMap.
- FastMap supports the Microsoft Office .xls and .xlsx formats.
- User access is based on the role template assigned to a user or group. For details about role templates, see [“Role templates” on page 113](#).
- For Long String data types, the medium text subtype is the only subtype supported for FastMap uploads. Fields with a large subtype are ignored by Excel and FastMap as these fields might be too large for Excel to store in a cell (the maximum storage for a cell is 32 KB).
- Fields that cannot be modified, such as the system **Creation Date**, **Created By**, or **Last Modified By** fields, also cannot be edited by using the FastMap process. For example, if you are migrating data, you cannot preserve the creation date information by using FastMap. FastMap import is not supported for the system Comment field.

The FastMap data validation process

When a FastMap template is imported into the IBM OpenPages with Watson application, FastMap checks the user profile, and the setup and format of the worksheets.

By default, FastMap uses the profile of the logged-on user to determine which object types and fields are valid. For example, if an object type or certain object fields are included in a data load template but are excluded in a user's profile, then that object type or those object fields will be excluded from the data imported by FastMap.

In general, FastMap uses the same validation rules that apply to data that is manually entered into the application. For example, validation errors would occur if the profile of the logged-on user includes required fields that are missing from the worksheet, or the maximum number of characters allowed for a field is exceeded, and so forth.

For more details about validation, see [“Resolving FastMap validation errors” on page 920](#).

FastMap localization

By default, FastMap uses the locale of the logged-on user to validate data in templates.

As a result, all data in FastMap templates, such as column headings, text, enumerated drop-down or multivalued selection field values, should be localized in the locale of the end user. For example, an end user with the Italian locale (it_IT) setting should only import FastMap templates with localized Italian values.

You can override the locale of the end user by explicitly specifying a locale in the Definition worksheet of a template. For example, if you specify the `locale` parameter as `en_US` and localize the template in English, the Italian user could upload the template for validation in English, not Italian. For more information, see [“Using the FastMap Definition worksheet” on page 934](#).

When you export object type data from the IBM OpenPages with Watson application, the locale is automatically set on the Definition worksheet.

Validation messages that are displayed by FastMap during processing can be localized through application strings.

FastMap can be accessed in both user interfaces

FastMap import and export functionality can be accessed in either the Task Focused UI or the Standard UI.

Files that are imported in one interface are immediately viewable in the other interface.

Accessing FastMap to import data and view status (Task Focused UI)

In the Task Focused UI, you can access FastMap to import data or check the status of your data imports. Importing object data using Fast Map is a two-step process consisting of validation and importing.

Before you begin

To access **FastMap Import** in the Task Focused UI, you must have the correct application permission set on your account. For more information about FastMap permissions, see [“Types of application permissions” on page 91](#).

Procedure

1. Click  > **FastMap Import**.

The **FastMap Import** tab displays a list of your imports. If you have the application permission to see imports performed by other users, you can click the **View** dropdown and select **All imports**. The **Created By** column is added to the grid if you select this view.

2. On the **FastMap Import** tab, click **Import**.
3. In the **FastMap validate and import** dialog box, click **Choose file** and select a file to import.
4. Click **Validate**.

You can either wait for the validation to complete or click **Close, we'll notify you** to be notified when the validation is complete. The notification contains a link to review the validation status messages. If you miss a notification message, you can click **View notification**  to see the message.

Results

If the validation fails, you are prompted to upload a corrected file.

If the validation completes with warnings, you have the following choices:

- You can upload a corrected file.
- If the warnings don't matter, you can import the object data.
- You can cancel and start the process from the beginning.

- You can close the dialog box. Later in the current session, you can view the notifications to see the list of warnings or return to the **FastMap Import** tab to import the file.

When validation completes successfully, you can choose to import or cancel.

When you choose to import, the progress indicator updates automatically. You can close the **FastMap import details** dialog box at any time and you will be notified when the import is complete.

Accessing FastMap to import data and view status (Standard UI)

In the Standard UI you can access FastMap in multiple ways from the **Reporting** menu to import data or check the status of your data imports.

Note: Access to FastMap depends on your permissions.

Tip: You can access FastMap in the Task Focused UI. For more information, see [“Accessing FastMap to import data and view status \(Task Focused UI\)”](#) on page 918.

Procedure

1. Log on to the OpenPages with Watson Standard UI.
2. Do one of the following to access FastMap:
 - Select **Reporting** on the menu bar and choose FastMap and one of the following reports listed in Table 276 on page 919.

Table 276. FastMap Reports	
Select this report...	To do this...
FastMap Import	Import data from a workbook template
My FastMap Import Status	View the status of all your data imports

- Select **Reporting** on the menu bar and choose **All Reports** from the list.
3. Navigate to the FastMap folder and, if necessary, expand the folder.
 4. Click the report you want (see Table 276 on page 919).

A separate browser window opens with the selected report.

Importing a FastMap data load template (Standard UI)

You can only view FastMap import jobs that you submit.

Procedure

1. Select the FastMap Import report to open it (for details, see [“Accessing FastMap to import data and view status \(Standard UI\)”](#) on page 919).
2. In the file selection box, type the name of the data import file, or click **Browse** to navigate to the file.
3. When finished, click **Import**.
4. If validation errors are detected, fix the errors in the workbook template.

For more information, see [“Resolving FastMap validation errors”](#) on page 920.
5. Resubmit the modified file for validation against the application:
 - a) In the **Import changes and revalidate** box, browse to or type the name of the modified file.
 - b) Click **Validate Changes**.
6. If validation errors are still detected, repeat Steps 4 and 5 until all the errors are resolved and no validation errors are displayed.
7. When finished and no errors are detected, click **Import Data**.

8. When the **FastMap Import Status** report window is displayed, use the **Refresh** icon to view the current status of the import (see [“Understanding import status messages”](#) on page 926 for more details).

Resolving FastMap validation errors

Before FastMap can import data into the IBM OpenPages with Watson application, all validation errors that are displayed in the FastMap Import window must be resolved.

You resolve these errors by opening the FastMap template in Microsoft Excel and modifying the data.

When finished, you must resubmit the updated template to FastMap for another validation check. If errors are still found, you must repeat the resolution process until all validation errors are resolved. After all validation errors are resolved, FastMap is ready to import the data into the OpenPages with Watson application.

Understanding FastMap validation errors

Validation errors and warnings are displayed as they occur in the FastMap Import window.

If the FastMap validation process completes with:

- No validation errors - a status message is displayed indicating the number of objects to be imported.
- Warnings - you can load your data or correct the warnings and revalidate.
- Errors - a "Validation Failed" status is displayed along with information about the error.

Table 277 on page 920 lists some of the most common messages that may be displayed in a FastMap Import window.

Table 277. FastMap import validation error information		
This column...	Displays this...	Possible values...
Type	The category of the message.	• Error • Warning
Description	The type of error, and the name of the missing or invalid object field or invalid value.	See “Troubleshooting FastMap validation messages” on page 921.
Sheet	The name of the object type worksheet.	For example, Processes or Risks.
Row	The row within the Excel worksheet containing the error.	The index number corresponding to a row, for example, 2.
Column Index	The column index within the Excel worksheet containing the error.	The index letter corresponding to a column, for example, N.
Column Header	The name of the column within the Excel worksheet containing the error.	The localized label of a field name, for example, Domain.

For example, if the following validation message was displayed in the table on the FastMap Import window:

```
Error Required property is missing value.(Domain) Processes 2 N Domain
```

You would open the data load template, and enter the missing value (such as Financial Management) in row 2 under the Domain column (N) on the Processes worksheet.

Troubleshooting FastMap conflict with recent updates warning message

If you are unable to import changes and this warning message is displayed: Record conflicts with more recent updates and will be ignored. You need to check the timestamp value for the exportDate parameter on the Definition worksheet in the template. The warning message is displayed whenever you try to import a template and the data for an object has been updated since the specified export timestamp.

Important: If you are certain that the changes you want to import are current for all objects in the workbook, you can remove the export timestamp from the template following this procedure.

Procedure

1. Open the FastMap template in Excel.
 - a) If necessary, unhide the Definition worksheet (see [“Unhiding a FastMap Definition worksheet” on page 935](#)).
 - b) Remove the exportDate parameter.
 - c) Save the change.
2. Resubmit the template for import.

Troubleshooting FastMap validation messages

FastMap Validation Messages contains a list of FastMap validation messages, a brief description of the cause of the message, and what a user can do to resolve the issue.

In the following two tables, [Table 278 on page 921](#) and [Table 279 on page 925](#), messages are listed in alphabetical order.

Table 278. FastMap validation error messages		
Message	Cause	Resolution
Currency field is missing currency code.	A local amount is entered but the Local Code field is blank.	Make sure a value is set for Local Code in currency fields.
Currency field is missing local amount.	A local code is entered but the Local Amount field is blank.	Make sure a value is set for Local Amount in currency fields.
Exchange rate for base currency can only be set to 1.	The Local Code and Base Code fields are set to the same value but the Exchange Rate field is set to a value other than 1.	If the Local Code and Base Code values are the same, set the Exchange Rate field to a value of 1.
Import of Signature Objects not supported.	Signature objects are not supported for import.	Remove Signature objects from the worksheet.
Invalid boolean format. Value must be either true or false.	An invalid Boolean value is specified.	Ensure the Boolean value is set to either true or false.
Invalid classifier format.	Values in classifier fields or classifier target fields were exported, edited, and re-imported.	Remove the value from the spreadsheet or re-export and import the data. Do not edit classifier fields or classifier target fields after exporting them.

Table 278. FastMap validation error messages (continued)

Message	Cause	Resolution
Invalid currency code.	An invalid value was entered for a currency code.	Ensure the 3-letter ISO currency code is spelled correctly and is valid.
Invalid date format.	The cell contents for a Date field are not recognized.	Format the cell in Excel as Date to resolve the issue. If you leave the format as either General or Text, the text in the cell must match the inputDateFormat parameter. You can set this on the Definition worksheet to values such as dd/mm/yy.
Invalid decimal format.	A non-numeric value was entered for a decimal field.	Make sure that decimal fields have a numeric value.
Invalid decimal range.	The numeric value entered is outside the minimum or maximum range defined for that field.	Make sure the specified value is within the numeric range defined for that field.
Invalid Exchange Rate.	Exchange rate is 0 or negative.	Make sure the exchange rate value is greater than 0 (zero).
Invalid group.	An invalid value was entered for a Group field.	Ensure the name of the group is spelled correctly and is valid.
Invalid Integer format	A non-numeric value was entered for a numeric value.	Make sure the field has a numeric value.
Invalid Integer range.	The numeric value entered is outside the minimum or maximum range defined for that field.	Make sure the specified value is within the numeric range defined for that field.
Invalid Object Profile. Unable to properly validate spreadsheet.	A value for the profile is specified that is not recognized.	Ensure the name of the profile is spelled correctly and is valid.
Invalid parent resource provided.	The value of the parentResource parameter is invalid.	Make sure the full path of the specified parent object is correct.
Invalid Property Type.	The column header is not recognized as a property by FastMap. Possible causes: • The field is misspelled in the column heading on the worksheet • The field is missing from the view of the profile being used to import data. The view is specified by viewName on the Definition worksheet. The default is Detail.	Ensure the column header is spelled correctly. If so, make sure the property is present in your profile's Detail View. Note: If you do not want the column to be processed, you can list it under the ignoreColumns parameter on the Definition worksheet.
Invalid URL.	An invalid URL was entered for a URL field.	Ensure the URL is correct and fully qualified.
Invalid user.	An invalid value was entered for a User field.	Ensure the name of the user is spelled correctly and is valid.

Table 278. FastMap validation error messages (continued)

Message	Cause	Resolution
Invalid user/group.	An invalid value was entered for a User/Group selector.	Ensure the name of the user or group is spelled correctly and is valid.
Locale is invalid.	The locale value specified is not recognized.	Ensure the value of the locale is spelled correctly and is valid.
Missing currency code column.	The local code column is missing and a local amount is specified.	Make sure the local Currency code column is present in your worksheet and has a value for this record.
Missing local amount column.	The local amount column is missing and a local code is specified.	Make sure the local Amount column is present in your worksheet and has a value for this record.
Multiple resources found with the same key value.	When using Key fields, a key is specified that is not unique and FastMap cannot determine which resource to update.	Make sure the value specified for each Key is unique.
Name cannot be blank.	An object type that is not configured for autonaming has an empty Name field or the Name column is missing from the worksheet. Note: This error will not occur if autonaming is enabled for an object type.	Make sure the Name column is present in your worksheet and has a value in it for this record.
Name contains illegal characters.	Name contains backslashes or forward slashes.	Remove any backward slash (\) or forward slash (/) marks from the name of the object.
Name exceeds maximum characters (in bytes).	Name is longer than 252 characters or bytes for multicode locales.	Make sure the name of the object is shorter than 252 characters or bytes.
Object cannot be associated to a parent of this type.	A parent-child relationship does not exist between the object types being associated.	Either enable an association between the object types you want to associate or modify the worksheet to reflect object types that have a child-parent association already configured.
Parent not specified.	A parent is not specified for a new object and the allowOrphans setting is not set to true. Objects being updated do not need to have a parent specified.	Ensure that all three parent fields are present and populated correctly.
Parent Resource content type not recognized. Check that it is viewable in your profile.	The object type of the resource specified by the parentResource parameter is not recognized.	Ensure the object type value is spelled correctly. If so, make sure the object type is present in your profile's Detail View.

Table 278. FastMap validation error messages (continued)

Message	Cause	Resolution
Parent Resource not found.	A parent is specified in your spreadsheet, but FastMap cannot find it in the IBM OpenPages with Watson repository.	Make sure that the Parent Path is pointing to the proper folder location and that the Parent Objects value is the proper name of the object.
Property value exceeds maximum characters.	A text field contains more characters than is allowed in the OpenPages with Watson application.	Modify the text field so it does not exceed the character or byte limit.
Required property is missing value.	A required field for the object type is missing a value. Possible causes: • The column is present on the worksheet and the cell is missing a value • The column for the required field is missing.	Make sure that you have a value set for all properties required on the object.
System error.	Any unexpected error occurred. Similar to a "Requested operation could not be completed" system error message.	Contact IBM OpenPages Support.
Text field formatted as number in spreadsheet.	A text property value is formatted as a number or a date in the spreadsheet. A Text field in OpenPages with Watson is formatted in the worksheet cell as Number or Date. The field cannot be read in by OpenPages with Watson in this state and maintain all of the Excel formatting.	Change the format of the cells in Excel to Text.
The file exceeds the maximum number of rows allowed for import.	The total number of rows in the workbook is greater than the value set in the Maximum Workbook Rows setting (see “Limiting the rows for import to optimize FastMap performance” on page 947).	Modify the worksheet so it does not exceed the row limit or change the value of the setting.
The value entered is not a valid selection for this field.	The value for a single select drop-down field is not a valid value. The value must be in the proper locale of the user for it to be recognized.	Ensure the value is typed correctly and is in the correct locale.
The value(s) entered are not valid selections for this field.	The value for a multi-select drop-down field is not a valid value. The value must be in the proper locale of the user for it to be recognized.	Ensure the value is typed correctly and is in the correct locale.

Table 279. FastMap validation warning messages

Message	Cause	Resolution
Full import will result in objects being deleted.	When setting fullImport to 'true', FastMap identifies objects to be deleted.	Informational message, no action required.
Invalid Content Type	The worksheet name is not recognized by FastMap as a valid object type in the system. Possible causes: - The object type is misspelled on the worksheet tab. - The object type is missing from the profile being used to import data. Although FastMap will import the workbook, the invalid worksheet will be ignored. - In an English locale, the data was exported to Excel. Afterwards, the locale in the Excel worksheet was change to something other than en_US. An error is issued when the data is imported with FastMap.	Make sure that the object type is spelled correctly on the tab of the worksheet. FastMap treats each worksheet in the workbook as a content type sheet. Note: If you do not want the worksheet to be processed, you can list it under the ignoreSheets parameter on the Definition worksheet.
Property is read only.	A value was entered for a field that is read-only in the view of the profile used for import. The view is specified by viewName on the Definition worksheet. The default is Detail. Although FastMap will import data, the read-only field will be ignored.	Remove the columns from your worksheet. You can also specify the ignoreReadOnlyWarnings parameter so that these messages do not occur. However, these fields will not be updated when importing.
Record conflicts with more recent updates and will be ignored.	A record's last modified date is more recent than the value from the exportDate parameter.	See “Troubleshooting FastMap conflict with recent updates warning message” on page 921 for details.

Viewing FastMap import status

Import status can be viewed in either the Task Focused UI or the Standard UI.

In the Task Focused UI, click  > **FastMap Import**. To access **FastMap Import**, you must have the correct application permission set on your account.

The **FastMap Import** tab displays a list of your imports. If you have the application permission to see imports performed by other users, you can click the **View** dropdown and select **All imports**. The **Created By** column is added to the grid if you select this view.

To see more information about a particular import, click the row for that import.

For information about viewing import status in the Standard UI, see [“Using the FastMap import status report window \(Standard UI\)”](#) on page 926.

Using the FastMap import status report window (Standard UI)

The FastMap Import Status report window in the Standard UI displays details about FastMap imports.

About this task

The FastMap Import Status report window does not automatically update the progress of the import and requires a manual refresh.

To understand the various status messages that may be displayed, see [“Understanding import status messages”](#) on page 926.

Important: Regularly check the status of your FastMap jobs to know if an import has successfully completed. Templates that have large amounts of data for import have long running processes. If services, for example, are restarted while FastMap import processes are still running, FastMap jobs will be terminated and the import will not be successful.

Tip: You can access FastMap in the Task Focused UI. For more information, see [“Accessing FastMap to import data and view status \(Task Focused UI\)”](#) on page 918.

The list in the FastMap Import Status report window is the same regardless of whether you access it in the Task Focused UI or the Standard UI.

Procedure

1. If the **FastMap Import Status** report window is not already opened, open the window. See [“Accessing FastMap to import data and view status \(Standard UI\)”](#) on page 919.
2. To view the current status of an import, click **Refresh** on the report.

Understanding import status messages

The FastMap Import Status report window displays a progress meter showing the percentage completed.

The information is listed in [Table 280 on page 926](#).

Table 280. FastMap Import Status Information		
This column...	Displays this...	Possible values...
Id	A job identifier.	A generated numeric value, for example: 547.
Name	The name of the import job.	FastMap Import
Status	A progress summary of the import.	• Running • Completed Successfully • Completed With Errors • Terminated (System)
Percent Complete	A progress meter showing the percentage completed	A numeric value, for example: 20%
Create Date	The date and time the import job was created.	A timestamp, for example: Sep 24, 2009 4:23:38 PM EDT

Table 280. FastMap Import Status Information (continued)

This column...	Displays this...	Possible values...
Message	The task detail of the import. Processing task messages contain such information as: • The start and end of the task • The type of task • The number and type of objects being processed • The number of objects created, modified, and unchanged	• Initialized • Preparing to create/update <number> resources • Objects being uploaded: <number> • Processing <number> <object-name> • Finished processing <number> <object-name> • Processed <number> rows • Upload Complete • Objects Created: <number> • Objects Updated: <number> • Objects with no changes: <number> • Terminated by system at startup • ERROR Sheet (object-name) <additional-detail>
Status	The status of each processing task that is displayed.	• Started • Running • Completed Successfully • Completed With Errors • Terminated (System)
Date	The start date and time of each processing task.	A timestamp, for example: Sep 24, 2009 4:23:42 PM EDT

For information about using the FastMap Import Status report window, see [“Viewing FastMap import status”](#) on page 925.

Creating FastMap import templates

The quickest way to create a FastMap data load template is to export data for an object type into a Microsoft Excel workbook.

You can use that workbook to modify the data, and then use FastMap to import the modified data into the IBM OpenPages with Watson application.

The data exported to a workbook by FastMap

When you export object data, the resulting Microsoft Excel workbook has the following characteristics:

- In the Standard UI, you can export either all object fields that are displayed on an object’s Detail View page or object fields that are currently displayed in the view you have open. The fields are exported to a corresponding worksheet in the workbook.
- In the Task Focused UI, all object fields for a given user profile are exported to a corresponding worksheet in the workbook.
- Each object field is represented by a column on the worksheet.
- The header row in the worksheet contains labels for each object field. However, if the `useSystemNames` export template parameter is set to `TRUE` or if duplicate labels exist in the current

locale, there are two header rows. The first header row contains full system names in the format, <Field Group>.<Field Name>, and the second header row contains labels for each object field.

For information about the useSystemNames export template parameter, see [“FastMap parameters for importing and exporting data” on page 937](#).

- The plural label of the exported object type is displayed on the worksheet tab in the workbook.

Note: For compatibility with Microsoft Excel, FastMap removes the following special characters from a plural label on the worksheet tab:

/ \ ? * : []

For example, if the localized plural label of Risk object types is /Risks10*, the tab on the exported worksheet would be Risks10.

- In the default (out-of-the-box) IBM OpenPages with Watson export template the special Delete column and the three Parent columns are hidden on the object type worksheet.

See [Table 281 on page 928](#) for details.

- The Definition worksheet is included in the workbook and populated, by default, with the profileName, locale, exportDate, and ignoreReadOnlyWarnings parameters.

See [“Using the FastMap Definition worksheet” on page 934](#) for details.

FastMap exported spreadsheet file name characters

When you export object data for an object type, the file name of the exported spreadsheet is derived from the plural label of the object type. If the plural label of the object type contains special characters, these special characters may be removed from the spreadsheet file name by the operating system causing a mismatch between the object type label and the file name. Special characters in a file name are constrained to characters allowed by the operating system.

See the help topic "Rules for Naming Folders, Objects, and Files" for more information about special characters in names. To access the online Help system, log on to the IBM OpenPages with Watson application, then click the **Help** link. In the **Help** window, click **Getting Started** to expand the folder, then click **Rules for Naming Folders, Objects, and Files** to display the topic.

For additional information about special characters in the exported spreadsheet, see [“The data exported to a workbook by FastMap” on page 927](#).

Working with data load worksheets

A data load worksheet for an object type contains columns that identify the path and fields of objects (resources) of the same type for which you want to import change data into the IBM OpenPages with Watson application.

Defining paths for objects

Sample Worksheet for Process Objects lists the various worksheet columns that you use to define the path of an object.

- The path columns in [Figure 71 on page 933](#) must precede any object field columns that are listed in a worksheet.
- If you have set the parentResource parameter on the Definition worksheet, the columns in [Figure 71 on page 933](#) are optional.

Table 281. Columns that define the path of an object

This column...	Contains...
Folder Path	The path of an object.

Table 281. Columns that define the path of an object (continued)	
This column...	Contains...
Parent Path	The path of an object's parent folder.
Parent Object Types	The type of parent object to which the child object will be associated.
Parent Objects	The name of the parent object.

For a sample worksheet showing these columns, see [“Sample Processes worksheet”](#) on page 932.

Using special column headings

You can add special column headings to a FastMap data load worksheet to:

- Delete objects from the IBM OpenPages with Watson repository (see [“Deleting objects with FastMap”](#) on page 929)
- Disassociate objects (see [“Disassociating objects with FastMap”](#) on page 930)

Note:

- Adding a special column heading to a worksheet is optional.
- The special column headings and values must be localized.
- The values associated with special column headings are not case sensitive.
- Special column headings can be placed anywhere in a worksheet. Placing these columns at the beginning of a worksheet makes them easy to find later.

Deleting objects with FastMap

To delete objects from the IBM OpenPages with Watson application, add a Delete column to the data load worksheet.

To delete objects by using FastMap, first ensure that the **Common > Cascade Delete > Include Object Types** setting specifies at least one object type.

By default, the Delete column is present on the worksheet when data is exported from the OpenPages with Watson application. To see how the Delete column is used in an example, see [Figure 69](#) on page 933.

Table 282. Delete Column Values	
If the value is set to...	Then...
Y	Objects that are specified for deletion (that is, have a Y in their row under the Delete column) will be deleted from the OpenPages with Watson repository. Any objects associated with the specified object using the Cascade Delete > Include Object Types setting will also be deleted from the repository. After an object is deleted, it cannot be restored.
N or "blank" (no value specified)	The object will not be deleted. This value is set by default.

[Table 282](#) on page 929 shows the values for the Delete column.

Disassociating objects with FastMap

To disassociate objects within the IBM OpenPages with Watson application, add a Remove Association column to the data load worksheet.

See [Figure 69 on page 933](#) for an example.

Table 283. Remove Association Column Values	
If the value is set to...	Then...
Y	Child objects with a Y in their row under the Remove Association column will be disassociated from the specified parent object. A parent object is defined by placing information in the corresponding row of the child object for the following columns: • Parent Path • Parent Object Types • Parent Objects
N or "blank" (no value specified)	The object will not be disassociated. This value is set by default.

[Table 283 on page 930](#) shows the values for the Remove Association column.

Defining property fields for objects in FastMap templates

The number and type of object field columns in a FastMap template for an object type are optional and depend on the type of data you want to import.

Here are some general rules for defining object fields:

- Each object field that you want to update for a selected object type requires a separate column on the worksheet.
- You must use localized column names and values.
- All object field columns follow the path definition columns as described in [Table 281 on page 928](#).

For more information about working with object fields, see [“Guidelines for entering object data into FastMap templates” on page 930](#).

Guidelines for entering object data into FastMap templates

The following are some general rules you should follow when entering object data into a FastMap data load template.

Associating child objects

To associate child object to parent objects, use the following columns:

- Parent Object Types - This localized column identifies the type of parent to which you are associating the record. For example, Business Entity or Risk.
- Parent Objects - This localized column identifies the name of the parent object to which you are associating the record.

Auto-naming

FastMap can override auto-naming. If auto-naming is enabled for an object and the Name column is excluded or left blank, the system assigns a name. If auto-naming is enabled for an object and a value exists in the Name column, that value is imported as the name.

Currency fields

For each currency field that you include in your template, you must use a special column syntax that defines the local currency code, the amount, and exchange rate of that currency data.

Where:

<field name> in [Table 284 on page 931](#) represents the name of a currency field for a specified object.

Table 284. Column syntax for currency fields	
Use this column syntax...	To define...
<field name>.Amount	The amount based on the local currency code.
<field name>.Currency	The local currency code of the data being entered.
<field name>.Exchange Rate	The exchange rate to apply when calculating the value in the System Base Currency. Note: • This field is optional. • If an exchange rate is not specified in the template, it will use the default exchange rate set in the application. • When entering data where the Local Currency Code is the same as the System Base Currency Code, this column should not be populated.

Note: If the following currency-related fields are included on a worksheet, these fields will be ignored during import:

Base Amount (this is a derived value)

Base Code (this value is set globally)

Enumerated multivalued selection fields

When entering data for enumerated drop-down or multivalued selection fields, only localized values are valid.

Each selection value should be entered on a separate line within the same worksheet cell.

Note: To enter data for multiple values in the same worksheet cell, press the Alt+Enter keys simultaneously on your keyboard (after you type the value) to enter a Microsoft Excel line break.

For example, you have a multivalued enumerated field called "Domain" with the following selection values: Compliance, Operational, Technology, Financial Management, Internal Audit. [Figure 68 on page 932](#) shows how data containing multiple values for the "Domain" field might look in the worksheet.

M	N	O
	Domain	
	Compliance	
	Compliance	
	Internal Audit	
	Operational	
	Technology	
	Financial Management	
	Internal Audit	
	Compliance	
	Operational	
	Technology	
	Financial Management	
	Technology	

Figure 68. Sample Multivalued Selection Column with Values

Adding custom columns and worksheets to FastMap templates

You can add user-defined columns to a worksheet or user-defined worksheets to FastMap templates.

Each custom column that you add to a worksheet must have a heading name, and each custom worksheet that you add to a workbook must have a worksheet name.

So that FastMap does not try to validate any user-defined columns or worksheets, you must add the following parameters to the Definition worksheet:

- `ignoreColumns` - use for any user-defined columns and specify each heading name. For example, "column1;column2".
- `ignoreSheets` - use for any user-defined columns and specify the worksheet names. For example, "sheet1;sheet2".

See [“Using the FastMap Definition worksheet”](#) on page 934 for a sample Definition worksheet, and [“FastMap parameters for importing and exporting data”](#) on page 937 for additional parameters.

Sample Object worksheet for updating and creating objects

The sample Processes worksheet in [Figure 69 on page 933](#) and Risks worksheet in [Figure 70 on page 933](#) contain a combination of existing objects for update and the creation of new objects.

Sample Processes worksheet

The sample Processes worksheet in Sample Processes Worksheet shows the following:

- Column A, row 5 contains an existing Process object (Proc - B03) that will be disassociated from the Boston entity.
- Columns B through E define the path of the object.
 - Rows 3, 5, 6, and 7 contain existing Process objects that require updating. With the exception of Row 5 (an existing object that will be disassociated), Columns C, D, and E can remain blank for existing objects.
 - Rows 2 and 4 contain information for the creation of new Process objects. Path and parent object information is provided in Columns C, D, and E for each new object to be created.
- Columns F through Z represent object-specific fields.

	A	B	C	D	E	F	G
	Remove Association	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description
1		/North America/United States	/North America/United States	SOXBusEntity	United States	Proc-U02	Payroll
2		/North America/United States/Boston				Proc-B01	Payroll
3		/North America/United States/Boston	/North America/United States/Boston	SOXBusEntity	Boston	Proc-B02	Payroll
4	Y	/North America/United States/Boston	/North America/United States/Boston	SOXBusEntity	Boston	Proc-B03	Funds Transfer
5		/North America/United States/Boston				Proc-B04	Payroll
6		/North America/United States/Cleveland				Proc-C01	Payroll

Figure 69. Sample Processes Worksheet

Sample Risks worksheet

The sample Risks worksheet in the Sample Risks Worksheet shows the following:

- Column A, row 4 contains an existing Risk object (Risk-N01) under the North America entity. The Y in this column will result in Risk-N01 being deleted from the repository.
- Columns B through E define the path of the object. Notice the following:
 - Rows 2 - 6 contain existing Risk objects that require updating (notice that Columns C, D and E can remain blank for existing objects).
 - Row 7 contains information for the creation of a new Risk object (notice that path and parent object information is provided in Columns C, D and E).
- Columns F through Z represent object-specific fields.

	A	B	C	D	E	F	G
	Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description
1		/North America/United States/Boston				Risk-B01	Payroll
2		/North America/United States/Cleveland				Risk-C01	Payroll
3	Y	/North America				Risk-N01	Payroll
4		/North America/United States				Risk-U01	Payroll
5		/North America/United States/Boston				Risk-B02	Payroll
6		/North America/United States/Boston	/North America/United States	SOXControlObjective	CO-B01	Risk-B03	Payroll

Figure 70. Sample Risks Worksheet

Sample self-contained object worksheet

If you are adding self-contained objects, such as Processes in a Process-based security model, these objects must reside under their own folder. This folder must match the object name.

Important: You must specify the container folder for a self-contained object.

Table 281 on page 928 shows how to specify folder and parent paths for Process objects in a Process-based security model. In this example, the Process folder is named PR-200 and is appended after the Business Entity Boston folder.

Notice that the Folder Path column contains the name of the PR-200 Process folder.

	A	B	C	D	E	F	G	H
	Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description	Creation Date
1		/North America/United States/Boston/PR-200	/North America/United States/Boston	SOXBusEntity	Boston	PR-200	Payroll	

Figure 71. Sample Worksheet for Process Objects (Process Security Model)

Figure 72 on page 934 shows how to specify folder and parent paths for child Risk objects in a Process-based security model. Similarly, in this example, the Process folder is named PR-200

Notice that both the Folder Path and Parent Path columns contain the name of the Process folder, PR-200.

	A	B	C	D	E	F	G
1	Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description
2		/North America/United States/Boston/PR-200	/North America/United States/Boston/PR-200	SOXProcess	PR-200	Risk-200	Payroll

Figure 72. Sample Worksheet for Risk Objects (Process Security Model)

Sample Business Entity worksheet for creating a new business entity structure

The sample business structure in Sample Business Entity Structure shows three levels of business entities.

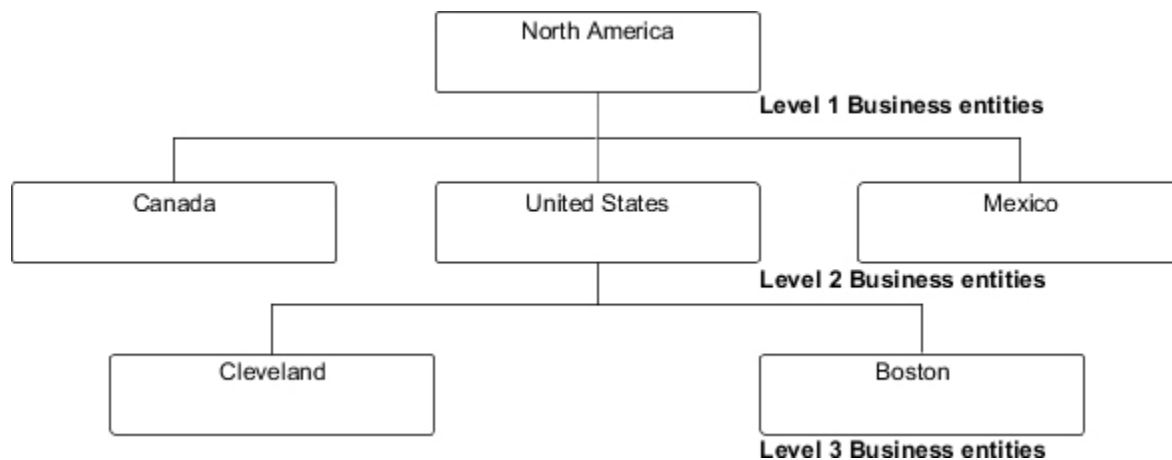


Figure 73. Sample Business Entity Structure

To create new Business Entity objects that map to the structure in [Figure 73 on page 934](#), you would create a Business Entities object worksheet in Microsoft Excel similar to the one shown in [Figure 74 on page 934](#).

The sample Business Entities worksheet in [Figure 74 on page 934](#) creates new entities and shows the following:

- Column A is an optional field that can be used to delete existing objects. Since all the objects in this worksheet are new, none are marked for deletion (by default, the value is N for no - do not delete).
- Columns B through E define the path of the new object. Notice that Row 2 contains the top-level Business Entity (North America), so the Parent Path and Parent Objects columns are blank.
- Columns F through Z represent object-specific fields.

	A	B	C	D	E	F	G	H
1	Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description	Entity Type
2		/North America		SOXBusEntity	North America	Global Headquarters		Headquarters
3		/North America/United States	/North America	SOXBusEntity	United States	North America - US		Region
4		/North America/United States/Cleveland	/North America/United States	SOXBusEntity	United States	Cleveland	Central Regional Sales	Region
5		/North America/United States/Boston	/North America/United States	SOXBusEntity	United States	Boston	Sales	Region
6		/North America/Canada	/North America	SOXBusEntity	North America	Canada	North America -	Sales Office
7		/North America/Mexico	/North America	SOXBusEntity	North America	Mexico	North America - Mexico	Sales Office

Figure 74. Sample Business Entity Worksheet

Using the FastMap Definition worksheet

You can include a Definition worksheet in a workbook to configure FastMap behavior.

When you export data from IBM OpenPages with Watson, by default the Definition worksheet is not hidden from users in the workbook, and does not have column headings.

By default, the following parameter values are set:

Table 285. FastMap Definition worksheet default parameters	
Parameter	Value
ignoreReadOnlyWarnings	TRUE
locale	en_US
profileName	Default
exportDate	The date and time the data was exported. Example: 24-Jul-2009 10:12:52 AM

Parameters that are listed in a Definition worksheet will override settings from other sources, such as JSP report parameters.

For more information, see [“FastMap parameters for importing and exporting data” on page 937](#).

Unhiding a FastMap Definition worksheet

If you do not see the Definition worksheet in a FastMap template workbook, and you want to change or add parameters to it, then you must unhide the worksheet.

By default, the Definition worksheet is not hidden.

Procedure

1. In Microsoft Excel, select the workbook with the hidden Definition worksheet.
2. From the toolbar select **Format | Sheet | Unhide**.
3. In the **Unhide** box, select **Definition** and click **OK**.
4. Save the file.

FastMap parameters

You can use FastMap parameters to customize how data is imported (uploaded) to and exported from the IBM OpenPages with Watson application.

To set FastMap parameters, you can do the following:

- List parameter names on the Definition worksheet of a FastMap template
- Pass parameters during an import through the FastMap JSP report page template (Standard UI only)

FastMap export templates

An export template is used to format object data exported into an Excel workbook.

By configuring parameters on the Definition worksheet of an export template, you can control the behavior of the export or its subsequent import.

Unless another template is specified, the IBM OpenPages with Watson application uses `DefaultTemplate.xls` as the default export template.

Modifying parameters in the default FastMap export template (Standard UI)

To add or modify parameters in the default export template, use the following steps.

Before you begin

To perform this procedure, you must have the **OpenPages Platform 3** profile associated with your username.

About this task

By default, the Definition worksheet in the `DefaultTemplate.xls` file has only the `ignoreReadOnlyWarnings` parameter set to `TRUE`. You can modify the template to include other parameters.

This video demonstrates how to add the `includeHTMLTags` parameter so that rich text formatting is preserved when you export (Standard UI):

<https://youtu.be/t1XT6hBp1aE>

Procedure

1. Go to **Administration > Manage System Files > Files**.
2. Double-click the row containing **DefaultTemplate.xls**.
3. Modify the `DefaultTemplate.xls` file, save it, and check it in. Available parameters are listed in [Table 287 on page 938](#).

Modifying parameters in the default FastMap export template (Task Focused UI)

To add or modify parameters in the default export template, use the following steps.

Before you begin

To perform this procedure, you must have the **OpenPages Platform 3** profile associated with your username.

About this task

By default, the Definition worksheet in the `DefaultTemplate.xls` file has only the `ignoreReadOnlyWarnings` parameter set to `TRUE`. You can modify the template to include other parameters.

Procedure

1. Click  > **System Configuration > System Files**.
2. Expand the **Templates > FastMap > FLV** folder and locate the `DefaultTemplate.xls` file.
3. Modify the `DefaultTemplate.xls` file, save it, and check it in. Available parameters are listed in [Table 287 on page 938](#).

Specifying a FastMap export template

The IBM OpenPages with Watson application supports multiple export templates.

You can specify export templates based on one or more of the following criteria:

- `ContentType`
- `Locale`
- `Profile`

Use the following rules when specifying criteria for an export template:

1. Criteria is specified in the name of the export template.
2. Each criterion is separated in the template name by a hyphen.
3. The criterion must be specified in order: `ContentType-Locale-Profile`

The system selects templates based on the following precedence: `ContentType -> Locale -> Profile`.

For example, SOXRisk.xls will be selected before DefaultTemplate-en_US-FCM Module.xls, and SOXRisk-All-FCM Module.xls will be selected before SOXRisk.xls

Note: If no match is found, the DefaultTemplate.xls export template is used.

The syntax for the export template name is:

```
<ContentType>-<Locale>-<Profile>.xls
```

Where:

<ContentType> is the system name of an object type (such as, SOXRisk), not the localized name. To specify all object types, use DefaultTemplate for the <ContentType>.

<Locale> is the language and locale code (for example, en_US). To specify all locales, use All for the <Locale>.

<Profile> is the name of a profile in the OpenPages with Watson application.

For purposes of illustration, the examples listed in [Table 286 on page 937](#) for specifying criteria in export templates use the Risk object type (SOXRisk) in the U.S. English locale (en_US) for users assigned the FCM Module profile.

Table 286. Example syntax for specifying criteria	
If you want to specify...	Example syntax...
a specific object type for a specific locale and profile	SOXRisk-en_US-FCM Module.xls
all object types (use DefaultTemplate) for a specific locale and profile	DefaultTemplate-en_US-FCM Module.xls
all locales (use All) for a specific object type and profile	SOXRisk-All-FCM Module.xls
all locales and all profiles for a specific object type	SOXRisk.xls
all profiles for a specific object type and locale	SOXRisk-en_US.xls
a specific profile for all object types and locales	DefaultTemplate-All-FCM Module.xls

Note: Subsets must honor ordering. For example, the following template names would be invalid:

FCM Module.xls - this is an invalid template name as the profile name must be the third criterion in the list (not the first).

en_US-FCM Module.xls - this is an invalid template name as the locale must be the second (not the first) and profile name must be the third (not the second) criterion in the list.

FastMap parameters for importing and exporting data

FastMap Definition Worksheet Import-only Parameters lists the various FastMap parameters that you can use on a Definition worksheet to configure FastMap behavior.

Table 287. FastMap Definition worksheet import-only parameters

Import-only Parameter Name	Default Value	Description
allowOrphans	FALSE	Determines if objects will be created when no parent object is specified. If the value is set to: • TRUE - creates an object if no parent is specified • FALSE - create an object only if a parent is specified
disableConflictDetection	FALSE	Determines if objects have been modified in the system since you last exported data into the worksheet. When a worksheet is exported from IBM OpenPages with Watson, it is marked with the time of the export. When data is imported back into the system, any objects that have been updated after this time will result in a validation message alerting the user and will not be updated. If the value is set to: • TRUE - no validation errors will be displayed and the worksheet values will override any recent changes in the system. • FALSE - a validation error will be displayed and the object will not be updated.
fullLoad	FALSE	Used when the data in your worksheet is a complete representation of what should be in the OpenPages with Watson repository. If used in conjunction with the parentResource parameter, only objects under that resource will be affected. Object types that are not being uploaded will not be deleted in the system. If the value is set to: • TRUE - any objects that are not in the set being uploaded will be deleted. • FALSE - any objects that are not in the set being uploaded will be retained.
ignoreColumns	null	Use if you want to include an additional column on a worksheet for information, and you want that column to be ignored by FastMap during validation. For example, "column1;column2"

Table 287. FastMap Definition worksheet import-only parameters (continued)

Import-only Parameter Name	Default Value	Description
ignoreEmptyFields	TRUE	Determines whether empty fields are blanked out during updates. If the value is set to: • TRUE - empty fields are ignored and not modified during an update. To explicitly clear a field, set its value to *blank*. • FALSE - empty fields will be blanked out during an update.
ignoreHiddenEnumWarnings	TRUE	Determines whether warning messages are displayed when values are submitted for hidden enumerated strings on a field in the OpenPages with Watson application. If the value is set to: • TRUE - no warning is displayed for hidden enumerated string values, whether changed or not. • FALSE - a warning is displayed for hidden enumerated string values, whether changed or not. Hidden enumerated string values that have been changed on objects will be updated during the import process regardless of the value of this setting.
ignoreReadOnlyWarnings	FALSE	If data is being uploaded into fields that are defined as read-only, OpenPages with Watson will display a warning message indicating that these values will be ignored. Use this setting to hide or display warning messages for read-only fields. Regardless of the whether warning messages are displayed, the data will not be uploaded. If the value is set to: • TRUE - warning messages are hidden. Note: This value is set to TRUE in the default template when you export data from OpenPages with Watson. • FALSE - warning messages are displayed.
ignoreSheets	null	Use if you want to include an additional worksheet for information, and you want that worksheet to be ignored by FastMap during validation. For example, "sheet1;sheet2".
parentResource	null	When set to the full path of an object, this parameter is used for all parent associations. All other parent information in the worksheet will be ignored.

Table 287. FastMap Definition worksheet import-only parameters (continued)

Import-only Parameter Name	Default Value	Description
shouldDefaultNotRequiredFields	TRUE	Determines whether default values will be used for all non-required fields that are missing values in a worksheet. If the value is set to: • TRUE - default values will be used for non-required fields that are missing values in a worksheet. • FALSE - no default values will be used for non-required fields that are missing values in a worksheet.
shouldDefaultRequiredFields	TRUE	Determines whether default values will be used for all required fields that are missing values in a worksheet. If the value is set to: • TRUE - default values will be used for required fields that are missing values in the worksheet. • FALSE - required fields that are missing values in the worksheet will display validation errors.
shouldValidateBESelector	TRUE	Determines whether Business Entity Selector display fields are validated during import. If the value is set to: • TRUE - a warning will be displayed for any business entity that does not exist. • FALSE - no validation will be done on Business Entity Selector fields. Warnings are displayed for incorrect or invalid values. For example, a warning is shown for a wrong value, such as a typographical error. In this case, you might not want to load the data. Warnings are also displayed in cases where a value changed making it currently invalid. For example, you exported data from OpenPages and then reimported the data later by using FastMap. The data can be flagged as invalid because a field value moved, was renamed, or been deleted. In this case, you might want to load the data because it was accurate in its original state.
shouldValidateRequiredFields	TRUE	Determines whether fields configured as required in the Profile are validated during import. If the value is set to: • TRUE - required fields will be validated. • FALSE - required fields will not be validated.
suppressWarnings	FALSE	Determines whether warning conditions will be displayed. If the value is set to: • TRUE - warning conditions will not be displayed. • FALSE - warning conditions will be displayed.

Table 287. FastMap Definition worksheet import-only parameters (continued)

Import-only Parameter Name	Default Value	Description
useFirstInstance	TRUE	Determines whether to use and validate only the first instance of an object when multiple instances of the same object are in a worksheet. If the value is set to: • TRUE - only the first instance of the object will be used to update the object. • FALSE - only the last occurrence of the object will be used to update the object.

Table 288. FastMap Definition worksheet import and export parameters

Import and Export Parameter Name	Default Value	Description
exportDate	null	When exporting data from OpenPages with Watson, this parameter is set, by default, to the current date and time. During the import validation process, each object is checked against the export timestamp. If changes to an object are more recent than the date and time of the export timestamp, a conflict exception warning message will be displayed during validation. The message alerts the user that they may be overwriting more recent changes made to an object. To disable this behavior you can set the disableConflictDetection parameter to TRUE.
headerRow	1	The row in the worksheet that stores the column headers.
locale	null	If a locale value is: • Not specified - the locale of the user will be used during validation. • Specified - the locale value that is set (such as, en_US, ja_JP, de_DE) will override the user's locale during validation.
multiSelectDelim	\r\n	Delimiter for multi-select enumeration lists. The default for Microsoft Excel is carriage return line feed that can be entered in Excel by using the Alt+Enter key sequence.
profileName	null	The name of the profile to validate against. If null, the profile of the currently logged-on user is used.

Table 288. FastMap Definition worksheet import and export parameters (continued)

Import and Export Parameter Name	Default Value	Description
useSystemNames	FALSE	By setting this parameter to TRUE FastMap will use the system names of the fields, not the localized labels, for column headers. System names are in the format [FIELD GROUP].[FIELD NAME]. For example, OPSSEnt.Domain. When exporting, the labels will also be included on another row as a convenience. The useSystemNames parameter has no effect on enumerated values or their localized labels.
viewName	null	Specifies the view definition that is used by FastMap to validate fields. Any fields that are loaded that are not in this view are reported as invalid. The value can be set to the following values: - the name of a Navigational View or Object View. The name is case sensitive. Fields specified as readonly are not imported. - PROFILE_FIELDS. If the field is in the user's profile, it will be imported, regardless of the view. If the value is null or invalid, or if an object type is missing from the view, the Detail View is used to validate fields instead.

This video demonstrates how to enable System Names as a header in all FastMap exports to prevent conflicts and errors during imports (Standard UI):

https://youtu.be/KGZwyaJBx_g

Table 289. FastMap Definition worksheet export-only parameters

Export-only Parameter Name	Default Value	Description
exportActorDisplayName	FALSE	If the value is set to TRUE, creates an additional <field_name>.Display Name column for actor fields. For example, an Executive Owner.Display Name column can be created for the Executive Owner actor field.
exportBaseAmount	TRUE	When exporting currency field data from OpenPages with Watson, this parameter determines whether to include a column for the Base Amount. If the value is set to: - TRUE - the Base Amount field is included. - FALSE - the Base Amount field is excluded.

Table 289. FastMap Definition worksheet export-only parameters (continued)

Export-only Parameter Name	Default Value	Description
exportBaseCode	TRUE	When exporting currency field data from OpenPages with Watson, this parameter determines whether to include a column for the Base Code. If the value is set to: • TRUE - the Base Code field is included. • FALSE - the Base Code field is excluded.
exportComputedFields	TRUE	Determines if computed fields will be evaluated and their values exported with other fields. If the value is set to: • TRUE - computed fields will be evaluated and their values exported with other fields. • FALSE - computed fields will be ignored during export.
exportExchangeRate	TRUE	When exporting currency field data from OpenPages with Watson, this parameter determines whether to include a column for the Exchange Rate. If the value is set to TRUE, the Exchange Rate field is included. If the value is set to FALSE, the Exchange Rate field is excluded.

Table 289. FastMap Definition worksheet export-only parameters (continued)

Export-only Parameter Name	Default Value	Description
exportParentInfo	PRIMARY	This optional parameter specifies whether the object parent information is included or excluded from the export. You can specify the value of TRUE, FALSE, or PRIMARY for this parameter. When this parameter is set to TRUE, the parent information is included in the export. The Parent Path, Parent Object Types, and Parent Objects columns are filled out in the target object worksheet. If an object in the worksheet has multiple parents, one row with the unique parent\folder information is included for each parent, and the object field information is repeated in each row for that object. The resulting FastMap format worksheet can be used to load the objects and their associations to another system that does not contain these object and association instances, but has the same configured object types and associations, fields, and profiles. The data on the loaded target system will be the same as on the source system from which the content was exported. However, the export performance is slower when this parameter is set to TRUE. When this parameter is set to FALSE, data for Parent Path, Parent Object Types, and Parent Objects columns is not exported. When this parameter is set to PRIMARY, is not specified, or has an invalid value on the Definitions worksheet, the Parent Path, Parent Object Types, and Parent Objects columns in the target worksheet are filled out only for the primary parent. If an object has multiple parents, the non-primary parents are not exported.

Table 289. FastMap Definition worksheet export-only parameters (continued)

Export-only Parameter Name	Default Value	Description
highlightDuplicates	TRUE	For objects with multiple parents, this parameter is used to display the duplicated parent information by using the light-gray, italicized font to de-emphasize this information. The values are TRUE or FALSE. This parameter is dependent on the useFirstInstance import parameter. When this parameter is set to TRUE, and the useFirstInstance parameter is also set to TRUE, the first instance of the object parent information is displayed using the standard font style, and the subsequent, duplicated information is de-emphasized. If useFirstInstance is set to FALSE, the last instance of the object parent information is displayed using the standard style, and the previous, duplicate information is styled based on the highlightDuplicates parameter. Styles that are inherited from the export template are maintained. When this parameter is set to FALSE, the style of the information for objects with multiple parents is unchanged. The files exported with the highlightDuplicates and useFirstInstance parameters can be imported through FastMap without changes if the user does not make any changes to the data in the worksheet. If there are multiple records for an object in the worksheet because multiple parents are exported, the only object from which updates are recognized by FastMap is based on the useFirstInstance parameter (default value TRUE).
includeHTMLTags	FALSE	Determines if HTML tags are exported for Rich Text Field formatted data. Rich Text Field data that is exported without HTML tags can be more easily read in the spreadsheet. However, if this field is updated and then imported into FastMap, the field will be imported as plain text as it has lost its formatting. If the value is set to: • TRUE - HTML tags are exported with the data. • FALSE - HTML tags are not exported with the data.

Configuring a lookup key for FastMap

If you are importing data from an external system, you can use a field other than the Name field to identify objects. Use the settings described in [Table 290 on page 946](#) to configure a lookup key for FastMap and set the scope of the lookup. This technique is most useful when you want to update data with existing records from an external system and synchronize it with records in OpenPages with Watson.

Note: You can only use object fields with the data type of Simple String, Integer, or Enumerated String as lookup keys.

For example, you want to import risk data from an external system into the OpenPages with Watson repository. Data from the external system has a unique ID field that you want to keep and use as a lookup key within OpenPages with Watson.

You would create a custom field group and field definition within OpenPages with Watson for the Risk object type (SOXRisk) for the ID field in the external system, for example, ExternalSys_A.Risk_ID.

You would then use the custom field group and field definition, ExternalSys_A.Risk_ID, to configure the Key setting for FastMap. After this setting is configured, you would add a column to your FastMap template for the Risk_ID field and populate it with values from the external system's ID field. When you import data from the external system, FastMap would then match records based on this field.

You can also scope the update of Risk data under a specific parent object. By setting the Scoped value to true, FastMap would only update objects under the parent that is specified in the worksheet.

Procedure

1. For each object type for which you want a lookup key, configure a field group and field definition (see Chapter 9, “Fields and field groups,” on page 199).
2. Configure the key fields settings for FastMap as follows:
 - a) Access the **Settings** page (see Chapter 19, “Viewing the Configuration and Settings page,” on page 597).
 - b) Expand the **Applications > GRCM > FastMap > Key Fields** folder hierarchy.
 - c) Navigate to the object type folder that you want and then expand the folder to see its settings.
 - d) For each object type for which you want to define a lookup key, modify the following settings as needed:

Table 290. Lookup key settings	
Setting Name	Description
Key	Used by FastMap to lookup objects when the name is not provided in a worksheet. Generally used in scenarios when objects are auto-named. The format is <pre>field_group.field_name</pre> Where: field_group is the name of the field group. field_name is the name of the object field. Example <pre>ExternalSys_A.R_ID</pre> If you have multiple fields, use a comma to delimit the fields. For example: <pre>field_group.field_name,field_group.field_name</pre>
Scoped	Used by FastMap to determine whether to lookup the value in the Key setting only under the parent objects or across all objects. If the value is set to: • true - the lookup is scoped only under parent objects. This is the default. • false - the lookup is not scoped and is across all objects.

- e) Click a setting to open its detail page.
- f) In the **Value** field, type a value.
- g) When finished, click **Done**.

The effect of the change is immediate.

3. In the FastMap template:

- a) For each field name that matches a <field name> value in the Key setting (from Step 2d), add a corresponding column to the template.
- b) Populate each corresponding column with values from your external system.
- c) When finished, import the template into FastMap.

Modifying export settings to optimize FastMap performance

Data is typically exported for an object type, modified, and imported back into FastMap.

To optimize and control the export of data, you can configure the following settings:

- **Maximum Export Size** - for details, see [“Maximum number of objects to export to Microsoft Excel on the Filtered List View”](#) on page 629.
- **Concurrent Exports** - for details, see [“Maximum concurrent export requests in the Filtered List View”](#) on page 632.

Limiting the rows for import to optimize FastMap performance

You can use the **Maximum Workbook Rows** setting to limit the number of rows that can be imported from a FastMap template.

By default, the value is set to 20000 rows (recommended maximum).

Note: Setting the number of rows for import above the recommended maximum of 20000 rows may result in slower performance and longer processing time. However, if you choose to set this value higher, then the processing timeout value in the **Transaction timeout** setting should also be increased (see [“Setting a transaction timeout to optimize FastMap performance”](#) on page 948 for details).

If the number of rows being imported exceeds the set value, then a validation error will be displayed stating that the workbook exceeds the allowable size.

For example, if the Maximum Workbook Rows setting has a value of 2500 and a user wants to import data into IBM OpenPages with Watson for Risk and Control objects, the workbook for the FastMap template contains:

- a worksheet for Risk objects with 1,000 rows of data
- a worksheet for Control objects with 2,000 rows of data
- a Definition worksheet with 5 rows of data

The total number of rows with data in the workbook is 3,005. Since the workbook exceeds the allowable size, a validation error will be displayed to the user.

Procedure

1. Access the **Settings** page (see [Chapter 19, “Viewing the Configuration and Settings page,”](#) on page 597).
2. Expand the **Applications > GRCM > FastMap** folder hierarchy.
3. Click the **Maximum Workbook Rows** setting to open its detail page.
4. In the **Value** field, type a number greater than zero (for example, 2500).
5. Click **Done**.

Setting a transaction timeout to optimize FastMap performance

If you set the value in the **Maximum Workbook Rows** setting above the recommended maximum of 20000 rows, you can use the **Transaction timeout** setting to increase the maximum time a process can run before it times out and stops.

By default, the value is set to 7200 seconds (2 hours).

Procedure

1. Access the **Settings** page (see [Chapter 19, “Viewing the Configuration and Settings page,”](#) on page 597).
2. Expand the **Applications > GRCM > FastMap** folder hierarchy.
3. Click the **Transaction timeout** setting to open its detail page.
4. In the **Value** field, type a number greater than 7200 (the value represents seconds).
5. Click **Done**.

Adding a processing delay to optimize FastMap performance

To reduce the processing impact of FastMap data imports on a system, you can use the **Process Delay** setting to set a delay in milliseconds between each record. If a value is set, the time to process the imported data will be extended.

By default, the value is set to 0 (zero).

Procedure

1. Access the **Settings** page (see [Chapter 19, “Viewing the Configuration and Settings page,”](#) on page 597).
2. Expand the **Applications > GRCM > FastMap** folder hierarchy.
3. Click the **Process Delay** setting to open its detail page.
4. In the **Value** field, type a number greater than zero.
5. Click **Done**.

Securing FastMap import templates stored on the server

You can use the **Encrypt FastMap Files** setting to configure security on FastMap import templates that are stored on the server.

By default, the value is set to `true`, which encrypts FastMap import templates stored on the server.

Note: Before you change the value of the **Encrypt FastMap Files** setting, check the status of FastMap import jobs to verify that no FastMap imports are pending processing. For more information about checking import status, see one of the following topics:

- For the Task Focused UI, see [“Viewing FastMap import status”](#) on page 925
- For the Standard UI, see [“Using the FastMap import status report window \(Standard UI\)”](#) on page 926.

If you change the value of this setting while FastMap processes are pending, the import will fail even if it the templates have passed data validation.

Procedure

1. Access the **Settings** page (see [Chapter 19, “Viewing the Configuration and Settings page,”](#) on page 597).

2. Expand the **Applications > GRCM > FastMap** folder hierarchy.
3. Click the **Encrypt FastMap Files** setting to open its detail page.
4. In the **Value** field, type one of the following values.

If the value is set to:

- **true** - FastMap import templates are encrypted when stored on the server. This is the default.
- **false** - FastMap import templates are not encrypted when stored on the server.

5. Click **Done**.

Cleaning up FastMap import templates stored on the server

You can use the **Delete After Days** setting to configure the maximum number of days that a FastMap import template can remain on the server before it is automatically deleted.

FastMap import templates that will automatically be deleted from the server include templates that have:

- Finished processing - either successfully or with errors/warnings
- Exceed the maximum number of days specified in the **Delete After Days** setting. By default, this value is set to delete FastMap import templates after 1 day.

Note: A FastMap import template that is older than the default value of 1 day will be automatically deleted regardless of whether or not the template has completed processing. We recommend a higher value for this setting if you upload large amounts of data using FastMap import templates.

Procedure

1. Access the **Settings** page (see [Chapter 19, “Viewing the Configuration and Settings page,”](#) on page 597).
2. Expand the **Applications > GRCM > FastMap** folder hierarchy.
3. Click the **Delete After Days** setting to open its detail page.
4. In the **Value** field, type a number greater than zero. By default, this value is set to 1.
5. Click **Done**.

AFCON-generated FastMap template best practices

You can use a IBM OpenPages with Watson AFCON-generated FastMap template (in .xls or .xlsx format) to import data into the FastMap tool. If you use this template, you must add a Definition worksheet to the template for compatibility.

The Definition worksheet should contain the following parameters and values:

- `firstDataRow` = [The first row from where the data starts]. This value is typically set to 11 for AFCON-generated templates.
- `useSystemNames` = TRUE
- `profileName` = [The name of the profile you are importing into]
- `inputDateFormat` = [Your date format]

If the OpenPages with Watson AFCON-generated FastMap template uses synonyms that are inconsistent with the object strings in the application, you must include the Synonyms worksheet from `locale_support.xls` in your template. The worksheet must be labeled Synonyms, and you can specify the locale column to use by setting the `synonymsLocale` parameter on the Definition worksheet (see [“Using the FastMap Definition worksheet”](#) on page 934).

A missing Definition worksheet in an OpenPages with Watson AFCON-generated FastMap template will result in validation errors, such as:

- Invalid Property Type errors for every property. For example,

```
Invalid Property Type. (RiskAssessment.Name)
```

- Errors if autonaming is not enabled for an object type. For example,

```
Name cannot be blank
```

- Errors about the parent object if autonaming is enabled for an object type. For example,
Parent not specified. (EL_11419)

Using FastMap with questionnaire template and assessment objects

You can use FastMap to import and export questionnaire template objects and the content in sections, subsections, and questions. You can also use it to import and export the standard fields for questionnaire assessment instances. However, you cannot use it import or export content, for example, question answers, comments, and attachments, on questionnaire assessment instances.

About this task

You can import and export content for the following objects:

- Questionnaire templates
- Section template
- Subsection template
- Question template
- Questionnaire assessments (standard fields only)

The `Enumerated Answers` field in the questionnaire template stores single and multiple choice answers in JSON format. You cannot add this field to the object profile views. However, you can import and export it.

Every question in a questionnaire template has an internal identifier that is stored in the `ReportID` field. You can import a questionnaire template and leave the `ReportID` fields empty. You should then launch a program that uses the questionnaire template so that the system can assign `ReportID` values. The `ReportID` values are required for questionnaire templates and assessments to work correctly. In particular, when you copy answers from one questionnaire assessment to another, the systems requires the `ReportID` values to identify questions and their answers. For more information, see *Launching a program and copying answers* in the *IBM OpenPages with Watson User Guide*.

Example

A question has three possible answers: Yes, No, and N/A, without descriptions and scores:

```
[{"value": "Yes"}, {"value": "No"}, {"value": "NA"}]
```

A question has two answers, Yes and No, where both answers have descriptions and scores:

```
[{"value": "Yes", "score": 20, "description": "description for Yes"}, {"value": "No", "score": 30, "description": "description for Yes"}]
```

A question has three answers, Yes, No, and N/A, where Yes requires a comment, No requires an attachment, and N/A requires both:

```
[{"value": "Yes", "score": 20, "requires": ["comment"]}, {"value": "No", "score": 30, "requires": ["attachment"]}, {"value": "NA", "score": 40, "requires": ["comment", "attachment"]}]
```

Chapter 29. Configuring and generating the reporting framework

You can configure IBM OpenPages with Watson to use Cognos Analytics for your organization's reporting requirements.

The reporting framework

The reporting framework consists of Cognos framework models that are configured and generated in OpenPages. They support both relational and dimensional data used for creating reports in Cognos Analytics.

When you generate the reporting framework, packages for selected framework models are published to the Cognos server. Using the query subjects and query items in these namespaces, report authors can create reports from within IBM OpenPages with Watson.

For more information about the relational and dimensional data models, see the *IBM OpenPages with Watson Report Author's Guide*.

Note: In reference to Reporting Framework V6, V6 refers to the latest framework version, not to any specific OpenPages release number.

Framework models

Framework models are based on the OpenPages object model and define subsets of objects and relationships necessary for your reporting requirements.

Framework models include the following components:

- Metadata
- Labels
- Facts and dimensions (standard models only)
- Custom query subjects

The reporting framework contains one pre-defined framework model named `OPENPAGES_FRAMEWORK_V6`, which is used for the pre-defined reports that are supplied with OpenPages. In addition to the `OPENPAGES_FRAMEWORK_V6` framework model, you can create your own framework models. The ability to use multiple framework models allows you to target a framework model to specific solutions, user roles, or object profiles.

There are two types of framework models that you can create:

- Standard
- Basic

Both types support profile filtering and allow you to define the package name.

Standard framework models

Standard framework models are intended for advanced report writers with extensive knowledge of Cognos Analytics. Use this type of model for reports that require the more complex functionality that Cognos offers. The `OPENPAGES_FRAMEWORK_V6` framework model is a standard model.

Standard framework models have the following characteristics:

- Support facts and dimensions.
- Nest relationship and dimensional subnamespaces.

- Use the following namespace hierarchy:
 - **[package label] > [namespace] > [namespace]_REL**
 - **[package label] > [namespace] > [namespace]_DIM**
- Use extensive foldering for query subjects and data items.
- Contain query subjects for ancillary objects such as Enumerations and Relationships.
- Use complex field representations, for example, currencies have multiple data items for local and base amount.
- Represent recursive objects as multiple query subjects using recursive object levels.
- Provide secondary compliance objects, such as Files or Issues, as Stand Alone objects. Relationships to them must be built in reports.

Basic framework models

Basic models are intended for end users who do not have extensive knowledge of Cognos Analytics. Use this type of model for more simple reports that you want to allow your end users to create as they require.

Basic framework models have the following characteristics:

- Do not support facts and dimensions. The [namespace]_DIM sub-namespace is not created.
- Use the following namespace hierarchy:
 - **[package label] > [namespace]**

Query subjects are created in the root namespace. The [namespace]_REL sub-namespace is not created.
- Do not create ancillary query subjects for Enumerations, relationships, and so on.
- Generate recursive objects, for example, Business Entity, SubMandate, and SubProcess, as single query subjects.
- Generate recursive object Levels only for Business Entity objects.
- Remove system-level data items, for example, IS_PRIMARY, LATEST_VERSION, and so on.
- Use simplified field representations, for example, single data items for Currencies and Enumerations as Local Amount and Localized Value, respectively.

More information

To configure framework models, see the following topics:

- [“Configuring settings that apply to all framework models” on page 957](#)
- [“Configuring framework models ” on page 961](#)
- [“Configure reporting framework namespaces” on page 963](#)

Namespaces

A namespace uniquely identifies a collection of query subjects, their relationships, and other objects (such as calculations) that you can use for authoring reports.

The framework generator uses the definition of a namespace (which is defined in the IBM OpenPages with Watson user interface) to create a corresponding namespace in the framework model.

The namespaces in the OPENPAGES_FRAMEWORK_V6 framework model are used by the pre-defined reports that are supplied with OpenPages. If you make changes to the namespaces, it can affect the functionality of the reports and may cause them to fail to run. You can add your own namespaces to the OPENPAGES_FRAMEWORK_V6 framework model to uniquely identify a collection of query subjects and other objects (such as calculations) for satisfying your reporting requirements

If you define your own standard and basic framework models, you must define namespaces for them.

When you generate the Reporting Framework V6, the packages for selected standard framework models are published to the Cognos server with relationship and dimensional subnamespaces:

- [namespace]_REL — this relational namespace enables report authors to report on objects based upon their defined relationships. This type of model is often used in list reports that use mixed data (numeric, data, and string).
- [namespace]_DIM — this dimensional namespace is organized into facts and dimensions, and gives report authors access to the online analytical processing (OLAP) features that are available in Cognos.

When you generate the Reporting Framework V6, the packages for selected basic framework models are published to the Cognos server. Query subjects are created in the root namespace. Sub-namespaces are not created.

To configure namespaces, see [“Configure reporting framework namespaces” on page 963](#).

For more information about namespaces and the framework model, see the *IBM OpenPages with Watson Report Author's Guide*.

Facts and dimensions

Facts and dimensions are components of a dimensional data model. Dimensionally modeled data works well with crosstab and graphical reports (such as charts and maps).

Facts are fields with a numeric data type (such as Currency, Integer, Decimal) that can be aggregated and analyzed. For each fact that is selected for inclusion in the dimensional model, you can also use the **Fact Types** setting. It globally controls the types of aggregations that can be created for each configured fact field (see [“Configuring reporting framework fact types” on page 957](#)).

Dimensions include enumerated fields, date fields, and dependent picklists that can be used by report authors as business filters and grouping fields.

You can control which facts and dimensions are represented in the dimensional namespace for each object type that can be used by report authors in reports.

To configure facts and dimensions, see [“Configuring facts and dimensions” on page 966](#).

Recursive object levels

If you want reporting capability in the dimensional data model of the reporting framework, you can use recursive object types to create sets of levels that will be reflected in the reporting framework for use by report authors. For each recursive object type, you can define multiple object levels. For the Business Entity object type, you can also create multiple sets of recursive object levels with each set having a different number of levels.

For more information about the dimensional data model, see the *IBM OpenPages with Watson Report Author's Guide*.

A recursive object type can repeat itself indefinitely or until some set limit is reached. The following object types are recursive within the IBM OpenPages with Watson application:

- Business Entity (SOXBusEntity)
- Sub-Process (SOXSubprocess)
- Sub-Account (SOXSubaccount)
- Sub-Mandate (Submandate)

Recursive object levels allow you to create a representation of corporate data using common names for each level of the set thereby providing the report author with additional context for creating reports (see [Table 291 on page 954](#)).

When the Reporting Framework V6 is generated, all levels that have been defined for recursive object types are reflected in the dimensional data model of the reporting framework. These structures allow

report authors to create, for example, drill-down dimensional reports where users can progressively navigate through the levels to more detailed data.

For a finer level of control, you can also specify which recursive object level sets you want available in a given namespace (see [“Configure reporting framework namespaces”](#) on page 963).

Note:

- You cannot delete Level1 for non-entity recursive object types.
- If you remove or edit levels in a set, reports that used these levels will no longer run.

To configure recursive object levels, see [“Configuring business entity recursive object levels”](#) on page 970.

Example

A report author works for Global Financial Services (GFS), a large multinational bank, with an organizational structure that is comprised of many business functions and groups. The report author has a requirement to create reports so business users at GFS can assess the risks associated with various processes that go across the company's business units. GFS has its business organized around functions, divisions, departments, and units.

To return data about the various business processes and their associated risks for each organizational level of the business, you might create a new set of recursive object levels for the Business Entity object type called "Risk Assessment" with the following levels as shown in [Table 291](#) on page 954.

Table 291. Sample Recursive Object Levels		
Level number	Level name	Example Business Entity instance user data
1	Group	Global Financial Services
2	Global Function	Client Markets
3	Division	Asia
4	Department	Underwriting
5	Unit	Japan

In addition to defining the business levels of the organizational structure for the Business Entity object type, you need to determine which business entity should be the starting point for scoping the data. In this example, we want the reporting data to start at the Global Function level. In the "Starting Entity" field, you would type:

/Global Financial Services

When the reporting framework is updated, a new Risk Assessment folder with the corresponding level folders and query items is created in the OpenPages_Reports_V6 package under the GRC Objects > Business Entity folder for report authors to use when they create Cognos reports.

Rules for defining sets of recursive object levels

Rules apply to the definition of sets of recursive object levels.

- Business Entity — this is the only recursive object type where you can define multiple sets of recursive object levels with a different starting entity for each set. Sets of Business Entity recursive object levels can also be edited and deleted.

By default, no recursive object levels are predefined for Business Entity object types.

- All other recursive object types (Sub-Process, Sub-Account, Sub-Mandate) have only one set of recursive object levels that, by default, is predefined and cannot be deleted.

By default, each of these recursive object types (excluding Business Entity) have a predefined first level that cannot be deleted but can be renamed.

- Each set of recursive object levels for the Business Entity object type requires a name and a root path.
- The name of each user-defined level must be unique across all recursive object types.
- The names of sets and levels can be localized.

Triangle object relationships

A triangle object relationship exists when one child has two parents that are related to each other. To enhance report authoring capability, use the **Supported Triangle Relationships** setting to configure object types with triangle relationships in the Reporting Framework V6 relational data model. V6 refers to the latest framework version, not to any specific OpenPages release number.

Within the triangle, the "top" (parent 1) and "bottom" (child) object types are non-recursive, with the "middle" (parent 2) object type being recursive (such as Sub-Process).

A triangle relationship that includes two recursive object types is not supported.

For example, a report author has a requirement to create a Risk report that allows business users to assess risks associated with various processes and sub-processes within their company.

To provide the report author with easier reporting capability in the framework model, you could configure a triangle relationship between the non-recursive child Risk object and its two related parents: a non-recursive parent Process object and a recursive parent Sub-Process object type, as shown in [Figure 75 on page 955](#).

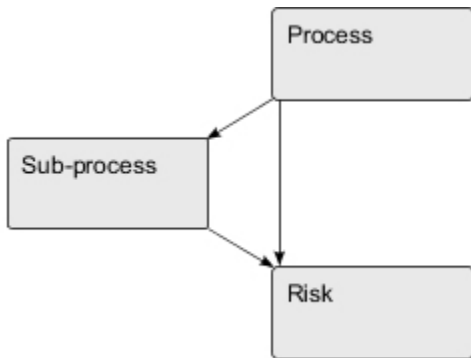


Figure 75. Triangle relationship between objects

The path between the objects forming a triangle relationship must be reflected in a namespace within the reporting framework. For example, a namespace might have the following object type hierarchy configured for Business Entity, Process, Sub-Process, and Risk object types as follows:

```
S0XBusEntity|S0XProcess,S0XProcess|S0XSubprocess,S0XSubprocess|S0XRisk
```

To reflect the triangle relationship shown in [Figure 75 on page 955](#), that namespace would have to be modified to also include the path between Process and Risk objects as follows:

```
S0XBusEntity|S0XProcess,S0XProcess|S0XSubprocess,S0XProcess|S0XRisk,
S0XSubprocess|S0XRisk
```

Without the configured triangle, the report author would have to use advanced techniques that may not perform as well to accomplish this task.

To configure triangle object relationships, see [“Setting the triangle reporting framework object relationships” on page 959](#).

Object type dimensions

Object type dimensions allow report authors to represent associations between object types as a dimension in the reporting framework to enhance report authoring capability in the dimensional data model. The object types do not have to be directly associated.

To configure object type dimensions, see [“Configuring object type dimensions”](#) on page 972.

Example

A report author works for Global Financial Services (GFS), a large multinational bank, with an organizational structure that is comprised of many business functions and groups. The report author has a requirement to create a report that shows aggregate test results and their associated controls for each division of the company.

The typical parent-child path in an object hierarchy between Business Entity and Test Result objects types is: Business Entity - Process - Risk - Control - Test - Test Result.

To skip object types in the hierarchy and create an association between Business Entity and Control objects, you could define an object type dimension called Entity-Control.

Since you already created a set of recursive object levels for the Business Entity object type (as shown in Table 291 on page 954), you could use the Division recursive object type level as a filter for the starting object type followed by the Control object type.

You can localize the name of the object type dimension for display in the reporting framework. If no translated text is provided, the value that is typed into the **Name** field for the object type dimension is automatically used.

When the Reporting Framework V6 is generated, the Entity-Control object type dimension would be available to report authors under the OBJECT_TYPE_DIMENSIONS folder in the DEFAULT dimensional namespace.

Selecting a starting object type for a dimension

Rules apply to the selection of an object type as a starting point for object type dimensions.

- Any object type can be selected as the starting object type.
- For the Business Entity object type, you can select a recursive object level as a starting point (for details on recursive object levels, see [“Defining business entity recursive object levels”](#) on page 970).

Planning the configuration

You can configure numerous aspects of the Reporting Framework V6.

Before you begin

Coordinate the configuration with your organization's Cognos report writers. Working together, you can ensure that the reports you are able to produce meet the needs of your organization. You can find detailed information about designing reports in the *IBM OpenPages with Watson Report Author's Guide*.

About this task

To configure the Reporting Framework V6, complete the following tasks:

Procedure

1. Review the OPENPAGES_FRAMEWORK_V6 framework model and namespaces. You may need to update the namespaces delivered with the system or create new ones to meet your requirements.
2. Review the registry settings that apply to all framework models. For information, see [“Configuring settings that apply to all framework models”](#) on page 957.

3. Configure your own framework models and namespaces. For information, see [“Configuring framework models”](#) on page 961.
4. Configure facts and dimensions. For information, see [“Configuring facts and dimensions”](#) on page 966.
5. Configure recursive object levels. For information, see [“Configuring business entity recursive object levels”](#) on page 970.
6. Configure object type dimensions. For information, see [“Configuring object type dimensions”](#) on page 972.
7. Generate the Reporting Framework V6. For information, see [“Generating the reporting framework”](#) on page 974.
8. Make reports available to end users by adding them to the home page tabs. For information, see [“Displaying Cognos reports on home page tabs”](#) on page 1112.
9. Optional: Configure Cognos dashboards and stories and make it available to end users by adding it to the home page. For information, see [“Creating a dashboard or story page \(Task Focused UI\)”](#) on page 177.

Configuring settings that apply to all framework models

The settings in the **Platform > Reporting Framework V6 > Configuration** folder apply to all framework models.

Configuring the number of models that can be concurrently generated

The Concurrent Models setting controls how many framework models can be concurrently generated.

Generating multiple models concurrently can improve the performance of the generation process. During generation each concurrent model uses memory and CPU resources on the Cognos Analytics server. Validate the impact and use caution before you increase this setting.

Platform > Reporting Framework V6 > Configuration > Concurrent Models

Default: 2

Values: In the **Value** field, type a number.

Configuring reporting framework fact types

A fact is a numeric field that can be aggregated.

For each fact that is selected for inclusion in the dimensional model (see [“Facts and dimensions”](#) on page 953 for details), you can use the **Fact Types** setting to globally control the types of aggregations that can be created for each configured fact field.

Table 292 on page 958 lists the valid fact types that can be used for aggregation. When the reporting framework is generated, all the aggregation types specified in the **Fact Types** setting will be created for each fact selected for inclusion in the dimensional model. The aggregated facts are then grouped into a single measure dimension under each object type in the model where they were defined.

By default, the following fact types are configured: SUM,AVG.

Platform > Reporting Framework V6 > Configuration > Fact Types

Default: SUM, AVG

Values: In the **Value** field, type one or more of the following values.

Note: If multiple values are specified, you must separate each value with a comma (for example: SUM, MIN, MAX, AVG).

Table 292. Valid Fact Type Values	
Fact Type	Action
SUM	Totals the value of objects in the set.
MIN	Returns the smallest existing value of an object in the set.
MAX	Returns the largest existing value of an object in the set.
AVG	Adds all values in the set and then divides by the count of existing values.
MED	Returns the median value of objects in the set.
STD	Returns the standard deviation of objects in the set.

Including workflow fields

The Include Workflow Fields setting controls whether workflow fields are included when you generate the reporting framework.

If you do not use GRC Workflow, set Include Workflow Fields to false.

If you use GRC Workflow, set Include Workflow Fields to true to make workflow information available in the reporting framework.

For information about reporting on workflow instance data, see [“Reporting on information in workflow instances”](#) on page 550.

For more information about GRC Workflow, see [Chapter 15, “Configuring GRC Workflow,”](#) on page 495.

Platform > Reporting Framework V6 > Configuration > Include Workflow Fields

Default: true

Values:

- true - workflow fields are included when you generate the reporting framework.
- false - workflow fields are excluded when you generate the reporting framework.

Adding locale codes to the reporting framework

You can add locale codes to the IBM OpenPages with Watson Reporting Framework V6 so that they can be applied to localized reporting and reports.

Platform > Reporting Framework V6 > Configuration > Locales

Default: en_US

Values: In the **Value** field, type the following locale code values. Multiple values must be separated by a comma.

- en_US (U.S. English)
- de_DE (German)
- en_GB (U.K. English)
- es_ES (Spanish)
- fr_FR (French)
- it_IT (Italian)
- ja_JP (Japanese)
- pt_BR (Brazilian Portuguese)
- zh_CN (Simplified Chinese)
- zh_TW (Traditional Chinese)

Defining the sort order locale

The Sort Order Locale setting controls the language in which query subjects and data items are sorted.

Multiple locales can be loaded into the reporting framework but the reporting framework has a static sort order based on the Sort Order Locale setting.

Platform > Reporting Framework V6 > Configuration > Sort Order Locale

Default: en_US

Values: In the **Value** field, type one of the following locale code values:

- en_US (U.S. English)
- de_DE (German)
- en_GB (U.K. English)
- es_ES (Spanish)
- fr_FR (French)
- it_IT (Italian)
- ja_JP (Japanese)
- pt_BR (Brazilian Portuguese)
- zh_CN (Simplified Chinese)
- zh_TW (Traditional Chinese)

Setting the triangle reporting framework object relationships

To enhance report authoring capability, use the **Supported Triangle Relationships** setting to configure object types with triangle relationships in the Reporting Framework V6 relational data model.

For more information, see [“Triangle object relationships” on page 955](#).

Platform > Reporting Framework V6 > Configuration > Supported Triangle Relationships

Default: none.

Values:

Important: The spelling and case of the object type name must exactly match its system name. For example, you would type SOXBusEntity for the Business Entity object type. Using the wrong case for letters or using the label text will result in an error message.

In the **Value** box, use the following syntax to configure the three objects in a triangle relationship:

```
Parent1|Parent2|Child
```

For example:

```
SOXProcess|SOXSubprocess|SOXRisk
```

Note: To enter multiple sets of triangle relationships, separate each triangle set with a comma as in:

```
SOXProcess|SOXSubprocess|SOXRisk,Mandate|Submandate|Requirement
```

Update the reporting schema to include the triangle relationship

After you've edited the triangle objects relationships, the reporting schema must be updated. You can either run the SQL script described in this procedure. This method incrementally updates the reporting

schema with the triangle relationship configuration. Or you can create the report schema using the application user interface method.

Tip: Run the following SQL script to incrementally update the reporting schema. This method is much faster than using the application user interface method.

Procedure

1. Log on to a machine with SQL*Plus and access to the database server.
2. Run the following script:

```
begin
    OP_CONTEXT_MGR.ENTER_SINGLE_USER_MODE;
    OP_RPS_TRIANGLE_MGR.ADD_TRIANGLE_SUPPORT;
    commit;
    OP_CONTEXT_MGR.EXIT_SINGLE_USER_MODE;
end;
/
```

What to do next

Regenerate the framework model. For details, see [“Generating the reporting framework ” on page 974.](#)

Enabling the reporting framework for custom forms

To run reports against a custom object type (such as a custom form or survey), you must include the object type in the **Object Prefix** setting with a unique two-letter identifier. The framework generator will use the two-letter identifier as a prefix when creating columns in the real-time reporting schema tables.

As a best practice, use Z<n> as a prefix for custom forms to avoid conflicts with future IBM OpenPages with Watson object types. Where: Z represents the first letter of the prefix, and <n> represents an uppercase letter, such as A, B, C, and so forth (for example, ZA, ZB, ZC).

Platform > Reporting Framework V6 > Configuration > Object Prefix

Default: none

Values: Add the new object type and prefix to the end of the current setting with a comma. The prefix must be entered as two uppercase letters, and must be unique; no other content type in the list can have the same prefix.

In the following example, the new object type (in bold) is called CustomSurvey and the prefix is 'ZA'.

```
...PROJECTACTIONITEM=PA,SOXSIGNATURE=SI,CUSTOMSURVEY=ZA
```

After you set these values, update the reporting framework model. For more information, see [“Generating the reporting framework ” on page 974.](#)

Defining the transaction timeout for reporting framework generation

The Transaction Timeout setting defines the processing timeout for the reporting framework generation process.

Platform > Reporting Framework V6 > Configuration > Transaction Timeout

Default: 21600

Values: The value is in seconds.

Configuring framework models

Settings in an **Platform > Reporting Framework V6 > Models > [model name]** folder define one framework model. You can have multiple framework model folders.

For information about framework models, see [“Framework models” on page 951](#).

Creating a framework model and namespace using a template

You can use the Template_Model framework model to quickly create new framework models and namespaces.

Before you begin

Verify that the **Allow Create and Delete Settings** setting is enabled. See [“Custom settings” on page 633](#).

About this task

The template model contains default values for settings and one namespace, TEMPLATE_NAMESPACE. To use it, you make a copy of the Template_Model folder and modify the settings to meet your needs.

Procedure

1. Click  > **System Configuration > Settings**.
2. Click **Platform > Reporting Framework V6 > Models**.
3. Select the **Template_Model** folder.
4. Click **Copy To**.
The **Copy Folder To** pane opens.
5. Enter the name of the new model in **Name**. Follow the naming guidelines in [“Naming framework models” on page 961](#).
6. Select a folder in **Target Folder**.
7. Click **Done**. The new folder is created.
8. Open the new framework model folder and change the **Package Label**. Review the other registry settings and change them to meet your requirements.
9. Expand the **Namespaces** folder in the new framework model folder. Expand the **TEMPLATE_NAMESPACE** folder. Review the namespace registry settings and change them to meet your requirements.

Defining a name for a framework model

Each folder under **Platform > Reporting Framework V6 > Models** defines one framework model. The name of the folder is the name of the framework model.

The name of the OPENPAGES_FRAMEWORK_V6 framework model folder cannot be changed.

Platform > Reporting Framework V6 > Models > [model name]

Default: none

Values: the name for the new framework model.

The newly created framework model is represented by a folder icon under the **Models** folder.

Naming framework models

The following list contains best practices to keep in mind when naming framework models:

- Framework model names are not translated in application text.
- Use the following characters when naming framework models:

- Lowercase letters
- Uppercase letters
- Numbers
- Underscores (_)

Examples : Audit_Model and RiskAssessment_Model

- Do not use spaces.

Defining the format for a framework model

The Format setting controls whether a framework model uses the standard or basic format.

For information about framework models, see [“Framework models” on page 951](#).

The Format setting of the OPENPAGES_FRAMEWORK_V6 framework model is standard. It cannot be changed.

Platform > Reporting Framework V6 > Models > [model name] > Format

Default: standard

Values:

- standard - the framework model uses the standard format
- basic - the framework model uses the basic format

Enabling a framework model

The Is Enabled setting controls whether a framework model is available for selection when you generate the reporting framework.

Platform > Reporting Framework V6 > Models > [model name] > Is Enabled

Default: true

Values:

- true - the framework model is available for selection when you generate the reporting framework.
- false - the framework model is not available for selection when you generate the reporting framework.

Defining the query mode for a framework model

The Mode setting controls whether a framework model is published in Cognos using Compatible Query Mode or Dynamic Query Mode.

The Mode setting for the OPENPAGES_FRAMEWORK_V6 framework model is cqm.

Platform > Reporting Framework V6 > Models > [model name] > Mode

Default: cqm

Values:

- cqm - the framework model is published in Cognos using Compatible Query Mode.
- dqm - the framework model is published in Cognos using Dynamic Query Mode.

Defining the package label for a framework model

The Package Label setting defines the package label name under which a framework model is published.

The Package Label setting for the OPENPAGES_FRAMEWORK_V6 framework model is OPENPAGES_REPORTS_V6. It cannot be changed.

Platform > Reporting Framework V6 > Models > [model name] > Package Label

Default:

Values: Type a name for the package label

Make package labels names meaningful to report writers.

Defining whether a framework model uses profile filtering

The Profile setting allows you to apply the filtering functionality of profiles to the data included in the reporting framework.

If an object type in the namespace is also in the profile given in the Profile setting, only fields listed for that object type in the profile definition are included in the framework. The ResourceId, Parent Folder Id, Reporting Period Id, and Detail Page URL fields are exceptions. They are always included.

If an object type in the namespace is not in the profile, all fields are included in the reporting framework.

If the Profile setting is empty, all fields are included in the reporting framework.

Platform > Reporting Framework V6 > Models > [model name] > [profile name]

Default:

Values: Type the name of a profile. Values are case sensitive.

Configure reporting framework namespaces

Settings in a **Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name]** folder define one namespace. A framework model can have multiple namespace folders. You can copy namespace folders from one framework model folder to another framework model folder. The same namespace folder name can be used in multiple framework models.

For information about namespaces, see [“Namespaces” on page 952](#).

The easiest way to create a new namespace is with the Template_Model framework model. For information, see [“Creating a framework model and namespace using a template” on page 961](#).

Defining a name for a reporting framework namespace

Each folder under **Platform > Reporting Framework V6 > Models > [model name] > Namespaces** defines one reporting framework namespace. The name of the folder is the name of the namespace.

The names of the system-supplied namespaces in the OPENPAGES_FRAMEWORK_V6 framework model folder cannot be changed.

Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name]

Default: none.

Values: name for the new namespace. For example, MYCOMPANY_NAMESPACE.

The newly created namespace is represented by a folder icon under the **Namespaces** folder.

Naming namespaces

Names of namespaces can be translated in application text. The following list contains best practices to keep in mind when naming namespaces.

- Keep namespace names short for readability (long names will wrap to another line).
- For consistency and compatibility with the reporting framework, use only the following characters when naming namespaces:
 - Uppercase letters
 - Numbers
 - Underscores (_)

Examples : MY_NAMESPACE and NAMESPACE101

- Do not use spaces.

Defining the object model for a namespace

The Object Model setting is required and contains the relationship path used for reporting in a namespace. A namespace cannot contain ambiguous paths.

The OpenPages with Watson Reporting Framework V6 generator uses the value pairs in this entry to define the parent-child relationships in the generated framework model.

Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Object Model

Default:

Values: In the **Value** field, enter value pairs to reflect parent-child object relationships. All parent-child paths must start with SOXBusEntity. The syntax is:

```
<parent object>|<child object>,<parent object>|<child object>
```

For example:

```
SOXBusEntity|SOXProcess,SOXProcess|SOXRisk,SOXRisk|SOXControl
```

System-supplied namespaces

If you change the **Object Model** setting in the system-supplied namespaces in the OPENPAGES_FRAMEWORK_V6 folder, it can affect the functionality of the pre-defined reports that are supplied with OpenPages.

Supported triangle relationships

If you want reporting capability for object types that are in a triangle relationship and have configured the **Supported Triangle Relationships** setting, the paths between these object types must be reflected in the **Object Model** setting of a namespace. The namespace can be either new or existing. For details on configuring the **Supported Triangle Relationships** setting, see [“Triangle object relationships” on page 955](#).

Configuring secondary compliance objects for basic framework models

If the namespace is used in a basic framework model, you must define allowed relationships between primary and secondary compliance objects in the **Object Model** setting.

- Secondary compliance objects relationships must be added to the Object Model registry entry for the namespace, for example, SOXBusEntity|SOXIssue.
- Multiple relationships can be defined for a secondary compliance object, for example, SOXBusEntity|SOXIssue,SOXProcess|SOXIssue.
- Relationships between secondary compliance objects must be explicitly defined, for example, SOXIssue|SOXTask.

When the reporting framework is generated:

- Secondary compliance objects are generated like other objects but will have a hyphenated name including their parent object, for example, Business Entity - Issue.
- A query subject is created for each relationship defined, for example, Business Entity - Issue, Process - Issue.
- Relationships between two secondary compliance objects are generated within the context of a primary compliance object. For example, SOXBusEntity|SOXIssue,SOXIssue|SOXTask generates as Business Entity - Issue and Business Entity - Issue - Action Item.

Setting a namespace as the default

The Is Default setting defines whether a namespace will be used as the default namespace in the OpenPages with Watson data model.

A framework model can have only one default namespace. In the OPENPAGES_FRAMEWORK_V6 framework model, the Is Default setting in the DEFAULT namespace is set to `true`.

Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Is Default

Default:

Values: In the **Value** field,

- `true` - the namespace is set as the default namespace for use by generation logic, and is created first.
- `false` - the namespace is set as a non-default namespace.

Enabling a namespace

The Is Enabled setting controls whether a namespace is generated when you generate the reporting framework.

Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Is Enabled

Default: `true`

Values:

- `true` - the namespace will be generated when the framework model is updated.
- `false` - the namespace will not be generated and any previously existing namespace will be removed.

Defining entity recursive object levels for a namespace

If one or more sets of recursive object levels are defined in the OpenPages with Watson application, the Entity Recursive Object Levels setting provides the ability to specify which recursive object level set you want available in a given namespace.

Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Entity Recursive Object Levels

Default:

Values: Multiple recursive object level sets must be separated by a comma. For example:

```
ROL-1,ROL-2,ROL-3
```

For information on defining recursive object levels, see [“Recursive object levels”](#) on page 953.

Defining whether facts and dimensions are enabled for a namespace

The Is Facts and Dimensions Enabled setting controls whether facts and dimensions are enabled for a namespace.

Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Is Facts and Dimensions Enabled

Default: `true`

Values:

- `true` - facts and dimensions are enabled for the namespace.
- `false` - facts and dimensions are not enabled for the namespace.

Configuring facts and dimensions

You configure facts and dimensions using the **Administration > Reporting Framework > Configuration** task in the Standard UI.

For more information, see [“Facts and dimensions”](#) on page 953.

Basic framework models do not support facts and dimensions. For more information, see [“Framework models”](#) on page 951.

The following table provides an overview of the configuration tasks for setting up facts and dimensions and a reference to the related information.

Table 293. Overview of configuration tasks for setting up facts and dimensions	
Task Description	Related Topic
For the selected object type, configure the facts you want available for reports in the dimensional namespace.	“Enabling and disabling facts” on page 966
If the object type has enumerated fields and dependent picklists, configure the dimensions you want in reports for these fields and picklists in the dimensional namespace.	“Enabling and disabling enumeration and dependent picklist dimensions” on page 967
You can configure the types of date dimensions you want available for reports in the dimensional namespace.	“Using date dimension types” on page 968
You can control whether facts and dimensions are enabled for individual namespaces.	“Defining whether facts and dimensions are enabled for a namespace ” on page 965
Update the Reporting Framework V6 to effect changes to facts and dimensions.	“Updating the reporting framework (Standard UI)” on page 978

Enabling and disabling facts

If an object type includes fields with a numeric data type (such as Currency, Integer, Decimal) then these fields are automatically listed in the Facts table for selection.

For example, fact fields for a Risk object type might include such fields as "Inherent Frequency" (a decimal data type field) and "Inherent Severity" (a currency data type field).

When regenerating the reporting framework to apply the changes made to fact fields, you can choose the "Dimensions and Facts" option. It regenerates and updates that portion of the reporting framework that changed.

Note: When you disable facts that were previously enabled, any reports that used these facts will no longer run.

Procedure

1. Complete one of the following steps to access facts and dimensions for an object type:
 - In the Standard UI, click **Administration > Reporting Framework > Configuration**. From the **Facts and Dimensions** pane, click the name of the object type to select.
 - In the Standard UI, click **Administration > Object Type**. Click the object type to select. From the **Facts and Dimensions** pane, click Edit.
2. Under the **Facts** table, do one of the following:

- To enable a fact, select the each fact to include in the reporting framework.
 - To disable a fact, disable each fact you want excluded from the reporting framework.
3. Click **Save**.

What to do next

Update the reporting framework to effect the changes. For information, see [“Updating the reporting framework \(Task Focused UI\)”](#) on page 977.

Enabling and disabling enumeration and dependent picklist dimensions

You can enable and disable enumerated fields and dependent picklists as dimensions.

If an object type includes fields with an Enumerated String data type, then these fields are automatically listed under the Enumerated Fields column in the **Enumeration and Dependent Picklist Dimensions** table for selection as dimensions. For example, enumerated fields for a Risk object type might include such fields as "Category" (a single value selection field) and "Domain" (a multivalued selection field).

All dependent picklists that have been defined in the application user interface (including any disabled picklists) for a selected object type are automatically displayed under the Dependent Picklists column in the **Enumeration and Dependent Picklist Dimensions** table.

Note:

- Disabling an enumerated field or dependent picklist that was previously enabled as a dimension will cause any reports that used these dimensions to no longer run.
- Enabling a dependent picklist as a dimension automatically enables the parent enumerated field, which is located in the same row as the dependent picklist. A dependent picklist cannot be enabled as a dimension without the parent enumerated field also being enabled.
- Disabling an enumerated field as a dimension will also disable all child dependent fields.
- If you disable a dependent picklist as a dimension, the parent enumerated field remains enabled.
- A dependent picklist that is disabled for an object type cannot be selected as a dimension.

Procedure

1. Complete one of the following steps to access facts and dimensions for an object type:
 - In the Standard UI, click **Administration > Reporting Framework > Configuration**. From the **Facts and Dimensions** pane, click the name of the object type to select.
 - In the Standard UI, click **Administration > Object Type**. Click the object type to select. From the **Facts and Dimensions** pane, click Edit.
2. Under the **Enumeration and Dependent Picklist Dimensions** table, complete one of the following tasks:

Table 294. Enumeration and Dependent Picklists tasks	
Task	Steps
Enable an enumerated field as a dimension	Under the Enumerated Fields column, select the box next to each enumerated field you want included as a dimension in the reporting framework.
Disable an enumerated field as a dimension	Under the Enumerated Fields column, clear the box next to each enumerated field you want excluded as a dimension from the reporting framework.

Table 294. Enumeration and Dependent Picklists tasks (continued)	
Task	Steps
Enable a dependent picklist as a dimension	- Under the Dependent Picklists column, select the box next to the picklist you want included as a dimension in the reporting framework. - In the same row as the dependent picklist, under the Enumerated Fields column, select the box next to the parent enumerated field if it is not already selected.
Disable a dependent picklist as a dimension	- Under the Dependent Picklists column, clear the box next to the picklist you want excluded as a dimension from the reporting framework. - In the same row as the dependent picklist, under the Enumerated Fields column, clear the box next to the parent enumerated field if not wanted as a dimension.

- Click **Save**.
- Update the reporting framework to effect the changes. For information, see [“Updating the reporting framework \(Task Focused UI\)”](#) on page 977.

Using date dimension types

When date fields are used as dimensions in reports, users can drill down through a date hierarchy from the year to a specific quarter, month, and/or day.

For date fields to be used as dimensions, you must first define a date dimension type then map that dimension to the date fields of an object type. The date dimension types that you define are globally available for all object type date fields.

You can localize the name of a date dimension type for display in the reporting framework. If no translated text is provided, the value that is typed into the **Name** field for a date dimension type is automatically used.

By default, the following system date fields are available under the Date Dimensions table for all object types but are not automatically configured with a date dimension type:

- Creation Date
- Last modification Date

Notice: If a system date field is configured with a date dimension type, it applies to all object types.

Adding a date dimension type

When you define a date dimension type, that dimension is available for selection on all date fields for any object type.

For more information, see [Table 295 on page 969](#).

Complete the following steps to add a data dimension type:

Procedure

- In the Standard UI, click **Administration > Reporting Framework > Configuration**.
- On the **Date Dimensions Type** table, click **Add**.

3. In the **Name** field, type a name for this date dimension.
4. Optional: Localize the text of the **Name** field for display in the reporting framework as follows. If no localized display text is specified, the value in the **Name** field is used by default.
 - a) Click the **Translate** link.
 - b) In the **Translate** window, next to each language you want, type the localized text into the box.
 - c) When finished, click **Apply**.
5. Select a value next to each dimension you want for this date type. Only one value can be selected for each type of date dimension.

<i>Table 295. Date dimension types</i>	
Date type	Description
Year	Returns the calendar year of the field. Example: 2010
Quarter	Returns the quarter within the calendar year. Example: "Quarter" would return "3" for the month of August.
Month	Depending on the selection, will return either a numeric or text string for the month. Example: "Month of Year" would return "8" for the month of August.
Week	Depending on the selection, will return the number of the week for either the month, quarter, or year based on a starting criteria. Example: "Week of Year (Starts on Sunday)" would return "33" for August 18, 2010.
Day	Depending on the selection, will return either a numeric or text string for the day of the week, month, quarter, or year based on an optional starting criteria. Example: "Day of Year" would return "230" for August 18, 2010.

6. Click **Save**.
Map the date dimension to an object type date fields. See [“Mapping date dimension types to date fields” on page 969](#).

Mapping date dimension types to date fields

After you create a date dimension type, you can then map that dimension to one or more date fields for an object type.

Each column in the **Date Dimensions** table represents a defined date dimension type, and each row represents a date field for the selected object type.

Procedure

1. Complete one of the following steps to access facts and dimensions for an object type:
 - In the Standard UI, click **Administration > Reporting Framework > Configuration**. From the **Facts and Dimensions** pane, click the name of the object type to select.

- In the Standard UI, click **Administration > Object Type**. Click the object type to select. From the **Facts and Dimensions** pane, click Edit.
2. On the **Date Dimensions** pane, select date dimension types, for each date field in a row.
 3. Click **Save**.

What to do next

Update the reporting framework to effect the changes. For information, see [“Updating the reporting framework \(Task Focused UI\)”](#) on page 977.

Enabling, disabling, modifying, and deleting a date dimension type

When you disable or re-enable a date dimension type, that date dimension type is disabled or re-enabled for all date fields in any object type. You can modify a date dimension type after you create it. When you delete a date dimension type, that date dimension type is permanently removed from the system on all date fields for any object type and cannot be retrieved.

Note: When you disable, modify, or delete a date dimension type, any reports that used that date dimension type will no longer run.

Procedure

1. In the Standard UI, click **Administration > Reporting Framework > Configuration**.
2. In the **Date Dimension Types** pane, navigate to the row containing the date dimension type you want to disable or re-enable.
3. Under the **Actions** column in the same row for that date dimension type, click **Disable**, **Enable** or **Delete**. Or, make modifications and click **Save**.

What to do next

Update the reporting framework to effect the changes. For information, see [“Updating the reporting framework \(Task Focused UI\)”](#) on page 977.

Configuring business entity recursive object levels

For the Business Entity object type, you can define and delete sets of recursive object levels, and modify the levels within each set.

By default, the Business Entity object type does not have any predefined sets of recursive object levels.

When the Reporting Framework V6 is generated, all user-defined sets of recursive object levels are available to report authors under the GRC_OBJECTS|SOXBUSENTITY_FOLDER folder in the default dimensional namespace. In addition, this structure is also available in the administrator interface in IBM OpenPages with Watson when configuring object type dimensions (see [“Object type dimensions”](#) on page 956).

For more information, see [“Recursive object levels”](#) on page 953.

Defining business entity recursive object levels

You can create multiple sets of recursive object levels for generation in the Reporting Framework V6. V6 refers to the latest framework version, not to any specific OpenPages with Watson release number.

About this task

To do this task, you need the **SOX > Administration > Object Types** application permission.

Procedure

1. In the Standard UI, click **Administration > Object Types**
2. From the list of object types, click the **SOXBusEntity** (Business Entity) link to open its detail page.
3. Navigate to the **Recursive Object Levels** table and click **Edit**.
4. In the definition pane, do the following:

Table 296. Recursive Object Levels Definition Boxes	
In this box...	Do this...
Name	Type a name for this set of levels.
Description	Optionally, type a description of this set.
Starting Entity	Type the full path, beginning with a slash, to the starting Business Entity. Note: Optionally, you can use a single slash (/) to specify all top level (Level 1) business entities.
Level 1	Type a unique name for this level.

5. To add another level to this set, click the  (plus symbol) icon and type a unique name for this level. Repeat this step for each level you want to add to this set.

Note: To remove a level that was added, click the  (minus symbol) icon.

6. Optional: Localize the text for the names of the set and the text for levels for display in the reporting framework as follows.

Note: If no localized display text is specified, the values in the **Name** and **Level** fields are used by default.

- a) Click the **Translate** link.
 - b) In the **Translate** window, for the language you want, type the localized text into the box.
 - c) Click **Apply**.
7. To add another set, click **Add** and repeat Steps 4 - 6.
 8. Click **Save**.
 9. To specify which recursive object level set you want available in a given namespace, configure the Entity Recursive Object Levels setting (see [“Configure reporting framework namespaces” on page 963](#)).
 10. Update the reporting framework to effect the changes. For information, see [“Updating the reporting framework \(Task Focused UI\)” on page 977](#).

Deleting business entity sets of recursive object levels

You can delete a set of recursive object levels for a Business Entity

Note: When you delete a set of recursive object levels for a Business Entity, all the levels that have been defined for that set are deleted and any reports that used these levels will no longer run.

About this task

To do this task, you need the **SOX > Administration > Object Types** application permission.

Procedure

1. In the Standard UI, click **Administration > Object Types**
2. From the list of object types, click the **SOXBusEntity** (Business Entity) link to open its detail page.
3. Navigate to the **Recursive Object Levels** table and click **Edit**.
4. Navigate to the pane with the set you want to delete, and click the **Delete** link.

5. Click **Save**.
6. Update the reporting framework to effect the changes. For information, see [“Updating the reporting framework \(Task Focused UI\)”](#) on page 977.

Modifying recursive object levels

You can add and remove levels in a set for all recursive object types.

Note:

- You cannot delete Level1 for non-entity recursive object types.
- If you modify existing recursive object levels in a set, reports that used these levels will no longer run.

About this task

To do this task, you need the **SOX > Administration > Object Types** application permission.

Procedure

1. In the Standard UI, click **Administration > Object Types**
2. From the list, click the name of the recursive object type you want to modify.
3. On the **Recursive Object Levels** table, click **Edit**.
4. In the definition pane, make the required changes.

To add or remove levels, complete one of the following tasks:

Table 297. Add or remove levels	
Task	Steps
Add another level to the set	Click the  (plus symbol) icon and type a unique name for this level.
Remove a level that was added	Click the  (minus symbol) icon.

5. Click **Save**.

What to do next

Update the reporting framework to effect the changes. For information, see [“Updating the reporting framework \(Task Focused UI\)”](#) on page 977.

Configuring object type dimensions

You configure object type dimensions using the **Administration > Reporting Framework > Configuration** task in the Standard UI.

For more information, see [“Object type dimensions”](#) on page 956.

Adding object type dimensions

Use the following instructions to define object type dimensions for generation in the Reporting Framework V6. V6 refers to the latest framework version, not to any specific OpenPages with Watson release number.

Procedure

1. In the Standard UI, click **Administration > Reporting Framework > Configuration**.
2. On the **Object Type Dimensions** table, click **Add**.
3. In the **Name** box, type a name for this object type dimension.
4. Optional: Localize the text of the **Name** field for display in the reporting framework as follows.

Note: If no localized display text is specified, the value in the **Name** field is used by default.

- a) Click the **Translate** link.
 - b) In the **Translate** window, next to each language you want, type the localized text into the box.
 - c) When finished, click **Apply**.
5. In the **Description** box, optionally type some descriptive text.
 6. Click the **Starting Object Type** arrow and select an object type or a recursive object level (if defined for Business Entity object types) from the list, then click **Go**.
 7. To add another object type to this dimension, do the following:
 - a) In the **Selected Object Types** table, under the **Actions** column, click the **Choose Object Type** link.
 - b) In the **Choose Object Type** window, select an object type then click **Apply**.
 - c) Repeat Steps a and b to add another object type to this dimension.
 8. Click **Create**.

What to do next

Update the reporting framework to effect the changes. For information, see [“Updating the reporting framework \(Task Focused UI\)” on page 977](#).

Modifying object type dimensions

You have the option to modify an object type dimension after you create it. Perhaps, for example, translated text needs to be modified or added, or a previously selected object type in a level needs to be changed.

Note: If you modify object types in an existing object type dimension, reports that used this object type dimension will no longer run.

Procedure

1. In the Standard UI, click **Administration > Reporting Framework > Configuration**.
2. From the list in the **Object Type Dimensions** table, click the name of the object type dimension you want to modify.
3. Make the changes you want (see [Table 298 on page 973](#)).

Table 298. Modifying an Object Type Dimension	
If you want to...	Then do this...
Change an object type	Click the Choose Object Type link for the object type you want to change and make another selection. Note: When you change an object type, all previously selected levels below that level are also deleted.
Delete a level	Click the Choose Object Type link for the object type level you want to delete and clear the selection box. Note: When you delete a level, all levels below that level are also deleted.
Change or add translation text for the Name field	Click the Translate link to open the Translate window.

4. Click **Save**.
5. Update the reporting framework to effect the changes. For information, see [“Updating the reporting framework \(Task Focused UI\)” on page 977](#).

Enabling, disabling, and deleting object type dimensions

You can disable and then re-enable an object type dimension at a later time. When you delete an object type dimension, that object type dimension is permanently removed from the system and cannot be retrieved.

Note: When you disable or delete an object type dimension, reports that used this object type dimension will no longer run.

Procedure

1. In the Standard UI, click **Administration > Reporting Framework > Configuration**.
2. In the **Object Type Dimensions** table, navigate to the row containing the object type dimension you want to disable, re-enable, or delete.
3. Under the **Actions** column in the same row for that object type dimension, do one of the following:
 - Click **Enable** or **Disable** (the link toggles between "Disable" and "Enable" depending on the selected action).
 - Click **Delete**.

What to do next

Update the reporting framework to effect the changes. For information, see [“Updating the reporting framework \(Task Focused UI\)” on page 977](#).

Generating the reporting framework

When you generate the Reporting Framework V6, the packages for all or selected framework models are published to the Cognos server with relationship and dimensional subnamespaces.

Overview

To generate the reporting framework, you can use either the Task Focused UI or the Standard UI. The functionality and results are the same regardless of which user interface you use. Status and refresh operations can be viewed in either user interface.

You can also use a command line tool. For more information, see [“Generating the reporting schema and framework from a command line” on page 164](#).

You should not use IBM Cognos Framework Manager to modify the packages. The packages are dynamically created and recreated when you launch the OpenPages Reporting Framework Generator. If you made changes using IBM Cognos Framework Manager, those changes are lost when you launch the OpenPages Reporting Framework Generator. If you would like to create a custom Cognos package, see your OpenPages Managing Consultant.

Regenerating the reporting framework

The following table lists the actions that require the reporting framework to be regenerated. In some cases, the reporting schema must also be recreated

<i>Table 299. Recreating the reporting schema and regenerating the reporting framework</i>		
This type of change...	Requires this to be regenerated...	
	Reporting schema	Reporting framework
Adding a new field to a field group.	No	Yes
Adding a new object type.	No	Yes

Table 299. Recreating the reporting schema and regenerating the reporting framework (continued)

This type of change...	Requires this to be regenerated...	
	Reporting schema	Reporting framework
Adding a new association between object types.	No	Yes
Removing object types or attributes. For information, see “Deleting a custom object type” on page 266.	Yes	Yes
Encrypting a long string (CLOB) field.	No	Yes
Enabling facts or dimensions.	No	Yes
Defining, modifying, or deleting business entity recursive object levels.	No	Yes
Removing a field from a field group.	No	Yes
Disabling an association between object types.	No	Yes
Disabling facts or dimensions.	No	Yes
Switching the security model. Note: Switching the security model after data is loaded or migrated into the system is not recommended and requires assistance from the OpenPages Professional Services team.	Yes	Yes
Changing the value of the Populate past periods setting. For information, see “Populating past reporting periods” on page 160.	Yes	No
Changing any setting used to compose URL links in the reporting schema, for example, the Host, Port, and Protocol settings. For information about updating the reporting schema, see “Updating URL host pointers for reports” on page 769 if you want to run the RPS_Update SQL script or “Creating or recreating the reporting schema (Task Focused UI)” on page 162 if you are update manually.	Yes	No
Adding an index to an RT_column by using the Settings > Platform > Reporting Schema > Create Index on Fields setting.	Yes	No
Configuring the triangles setting. For information, see “Triangle object relationships” on page 955.	Yes	No

Important: When you regenerate the reporting framework, you need to revalidate reports. Failing to do so may result in reporting errors.

Reporting framework permissions

Before performing any actions on a reporting framework, you must have specific application permissions set on your account.

For more information, see “Types of application permissions” on page 91).

Table 300. Reporting framework permissions	
This application permission...	Is used to...
Reporting Framework	Update all or selected components of the reporting framework. The Reporting Framework permission applies to both the Reporting Framework Generation task on the Administration menu in the Task Focused UI and the Administration > Reporting Framework > Generation task in the Standard UI.
Reporting Framework Configuration	Configure facts and dimensions using the Administration > Reporting Framework > Configuration task in the Standard UI.

Choosing update options in the reporting framework

When you generate the Reporting Framework V6, you can choose to update all or particular components of the reporting framework.

The Legacy Reporting Framework cannot be generated.

Table 301 on page 976 lists the various options for updating the reporting framework.

Table 301. Reporting Framework Generation Options	
This option...	Does this...
Framework Model	Generates the model in the relational model.
Facts and Dimensions	Generates the dimensions and facts in the dimensional model.
Custom Query Subjects	Generates any custom query subjects that are defined. For information about custom query subjects, see the <i>IBM OpenPages with Watson Report Author's Guide</i> .
Labels	Imports your object text into the reporting framework.
All Models	Generates the component you select (Framework Model, Labels, Facts and Dimensions, or Custom Query Subjects) for all framework models that are enabled.
Selected Models	Generates the component you select (Framework Model, Labels, Facts and Dimensions, or Custom Query Subjects) for selected framework models. The framework models must be enabled.

When you update the reporting framework, any changes to the reporting schema are reflected in Cognos. After the reporting framework model in Cognos is updated, report authors can create and modify reports based on these changes. If the reporting framework is not updated, external reports such as those built with Cognos will not be able to access the updated reporting schema.

You add two new fields to a Risk object type and add a new child or parent relationship to a Control object type. You also want users to be able to run reports that contain these new fields or relationships.

To make these changes available to a report author in the Cognos tool, you must update the reporting framework.

After the Cognos reporting framework is updated, a report author could then create new (or modify existing) reports that contained the new fields or relationships. For more information about the Cognos reporting framework, see the *IBM OpenPages Report Author's Guide*.

Updating the reporting framework (Task Focused UI)

After the reporting schema has been recreated, the reporting framework must be updated as well to propagate the changes to the Cognos reports.

About this task

To do this task, you need the **SOX > Administration > Reporting Framework**.

Procedure

1. Click  > **Cognos Analytics > Reporting Framework Generation**.
2. Click **Update**.
3. Complete the options on the Reporting Framework Generation page. For more information, see [“Choosing update options in the reporting framework” on page 976](#).
4. Click **Submit**.

What to do next

Review the results. For more information, see [“Viewing reporting framework details \(Task Focused UI\)” on page 977](#). Revalidate reports. Failing to do so may result in reporting errors.

Viewing reporting framework details (Task Focused UI)

You can view the details of a refresh operation and review errors, if they were encountered.

Procedure

1. Click  > **Cognos Analytics > Reporting Framework Generation**.
2. On the **Reporting Framework** tab, use the search to find the operation that you want to view.
3. Click the name of the operation.
A summary page opens with two tabs, **Information** and **Log**.
4. On the **Information** tab, you can view information about the operation.
5. If suboperations exist, they are listed in on the **Suboperations** pane.
 - a) To view suboperation details, click the name of the suboperation.
 - b) To view log details, click **View Log**.
6. On the **Log** tab, you can view log messages for an operation or suboperation.

Accessing the reporting framework (Standard UI)

To update components of the reporting framework or to configure facts and dimensions, you must access the reporting framework.

Before you begin

To update or configure the reporting framework, you disable System Administration Mode (for more information, see [“Enabling and disabling System Admin Mode” on page 71](#)).

Make sure the following application permissions are set on the user account. For information, see [“Reporting framework permissions” on page 975](#).

Procedure

Click **Administration > Reporting Framework**, and click one of the following:

- **Generation** — to update all or selected components of the reporting framework, such as metadata, labels, dimensions and facts, and custom query subjects for all or selected framework models.
- **Configuration** — to configure facts and dimensions, object type dimensions, and date dimension types.

Updating the reporting framework (Standard UI)

After the reporting schema has been recreated, the reporting framework must be updated as well to propagate the changes to the Cognos reports. Whenever you update the reporting framework, you need to revalidate reports. Failing to do so may result in reporting errors.

Note: This procedure assumes that you have created a new reporting schema.

About this task

Tip:

You can generate the reporting framework in the Task Focused UI. For more information, see [“Updating the reporting framework \(Task Focused UI\)”](#) on page 977.

Procedure

1. Access the **Reporting Framework Operations** page (see [“Accessing the reporting framework \(Standard UI\)”](#) on page 977).
2. Disable System Admin Mode if it is enabled. For more information, see [“Enabling and disabling System Admin Mode”](#) on page 71.
3. On the **Reporting Framework Operations** page, click **Update**.
4. In the **Reporting Framework Generation** window, complete the following steps:
 - a) Under **Framework Generation**, select the **Framework Model**, **Labels**, **All Models** or **Selected Models** options and any additional options for generation in the Reporting Framework V6 relational data model.
 - b) Click **Submit**.

You are returned to the Reporting Framework Operations page with the new task listed in the Reporting Framework Operations table.
5. To view the progress of the update, click **Refresh**. The Percent Complete column on the Reporting Framework Operations table updates the percentage of completion.

Viewing reporting framework operation details (Standard UI)

You can view the details of a refresh operation, including any errors that were encountered.

About this task

Tip:

You can view reporting framework operation details in the Task Focused UI. For more information, see [“Viewing reporting framework details \(Task Focused UI\)”](#) on page 977.

Procedure

1. Click **Administration > Reporting Framework > Generation**.
2. On the **Reporting Framework** tab, click the name of the operation that you want to view.
A summary page opens with two panes, **Operation Detail** and **Sub Operations**.
3. On the **Operation Detail** pane, click **View Log**.
The log message detail page appears.
4. If a sub-operations exists, they are listed in on the **Sub Operations** pane.

- a) To view sub-operation details, click the name of the sub-operation.
- b) To view log details, click **View Log**.

Chapter 30. IBM OpenPages with Watson connectors

You can leverage information from across the business by using connectors to collect information from third-party solutions.

IBM OpenPages with Watson connectors use IBM Security Directory Integrator (SDI) to pull data into OpenPages

Security Directory Integrator is a general-purpose integration tool that you can use to build integrations between multiple data sources and targets. Connectors must be imported into a Security Directory Integrator workspace. (IBM Security Directory Integrator is the latest name for IBM Tivoli® Directory Integrator.)

The version included in the IBM OpenPages with Watson installation media is Security Directory Integrator 7.2.0.3. This version is supported by the QRadar® integration package and by IBM OpenPages SDI Connector for UCF Common Controls Hub.



Attention: Security Directory Integrator must be at the 7.2.0.3 level.

IBM QRadar integration

IBM OpenPages with Watson includes an IBM QRadar integration package. QRadar is a separate stand-alone enterprise-level application. It is not included with IBM OpenPages with Watson.

IBM QRadar is a SIEM (Security Information and Event Management) system that contains relevant data for the Incident object type in OpenPages. In QRadar, this data is called an Offense.

Data can be pulled from QRadar, initiated by IBM Security Directory Integrator (SDI), then mapped one-to-one to Incidents in IBM OpenPages with Watson.

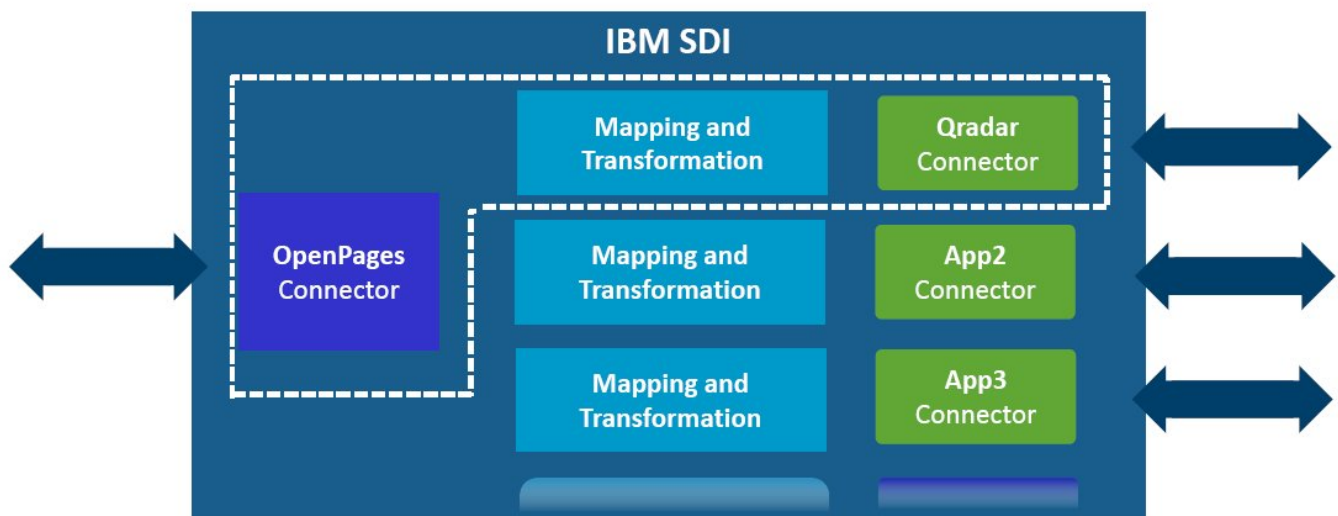


Figure 76. How OpenPages and QRadar work together

Using the QRadar integration project

The IBM QRadar integration project is an optional project that you can install to import Offenses from QRadar and create them as Incidents in the IBM OpenPages with Watson.

Before you begin

You must complete the following steps to install and configure the QRadar integration project before you begin. For more information, see "Installing QRadar integration" in the *IBM OpenPages with Watson Installation and Deployment Guide*.

About this task

Connectors are plug-ins for SDI that are reusable components. OpenPages has one connector developed for OpenPages functionality. The connector is generic to any OpenPages object type and field type.

You can use QRadar filtering so that the relevant subset of Offenses can be managed in the context of the impact on your business. For example, you can configure the connector to import only Offenses that are open, or based on the date.

The SIEM API documentation is available in the QRadar Console. This can provide guidance on what to specify for the filter and the fields, (specified by the **qradarFilter** and **qradarFields** properties in the `connector.properties` file).

Procedure

1. Ensure IBM QRadar is installed. IBM QRadar is a separate enterprise-level application. It is not included with OpenPages.
2. Install IBM Security Directory Integrator 7.2, then install pack 3. The installation files are available in the OpenPages installation media.
3. Configure Security Directory Integrator to connect to QRadar.
4. Configure the property files.
5. Deploy the assembly line.



Attention: The assembly line will not run when the OpenPages user that is configured to run the assembly line has left System Admin Mode enabled in OpenPages. You must ensure that System Admin Mode is disabled to run the assembly line. To disable System Admin Mode, click



> **Disable System Admin Mode.**

6. The results of running the assembly line show up as new or updated Incident objects. To view them, click **Events > Incidents** in OpenPages.

Configuring email notifications to be sent from the QRadar assembly line connector components

Both of the `QRadarOffensesToIncidents` assembly line connector components are able to send email notifications to alert people such as the IBM Security Directory Integrator (SDI) administrator when errors or exceptions occur during the execution of the `QRadarOffensesToIncidents` assembly line.

About this task

To enable this capability, the three SMTP properties in the `connector.properties` file must be configured. Then, when an error or exception occurs, in addition to the error-level message getting logged to the SDI log file or to the SDI console, an email with the log message is also sent to the email addresses configured in the SMTP **mailTo** property of the `connector.properties` file.

Email messages can be sent from either the QRadar API connector component or the IBM OpenPages with Watson connector component of the `QRadarOffensesToIncidents` assembly line. Also, the IBM OpenPages with Watson connector automatically sends warn-level messages if there are issues with the

validity of the primary parent ID supplied to the IBM OpenPages with Watson connector when attempting to create a new IBM OpenPages with Watson object. Updating an existing IBM OpenPages with Watson object does not require a primary parent ID to be specified.

Procedure

1. Configure the **mailTo** property of the connector .properties file.

The email address to use for sending email notifications about errors and exceptions that occur in the assembly line connectors. You can specify one or more email addresses by typing a comma-separated list. For example, **mailTo**=user1@acme.com,user2@acme.com.

2. Configure the **smtpPort** property of the connector .properties file.

The SMTP port to use for sending email notifications about errors and exceptions that occur in the assembly line connectors. The default port to use for an SMTP server is 25.

3. Configure the **smtpHost** property of the connector .properties file.

The SMTP host to use for sending email notifications about errors and exceptions that occur in the assembly line connectors. Specify either an IP name or IP address. For example, **smtpHost**=mySmtphost.acme.com or **smtpHost**=192.168.10.20.

Specifying a primary parent ID to the OpenPages connector

IBM OpenPages with Watson objects that are created by the OpenPages connector must have a primary parent ID.

Procedure

There are three ways to supply a primary parent ID to the OpenPages connector component, described in the order in which they are searched for:

- Provide the object resource ID of an existing suitable parent object as a string value in the **work.primary_parent_id** property in the output mapping:

The following graphic shows the **work.primary_parent_id** property in the output mapping:

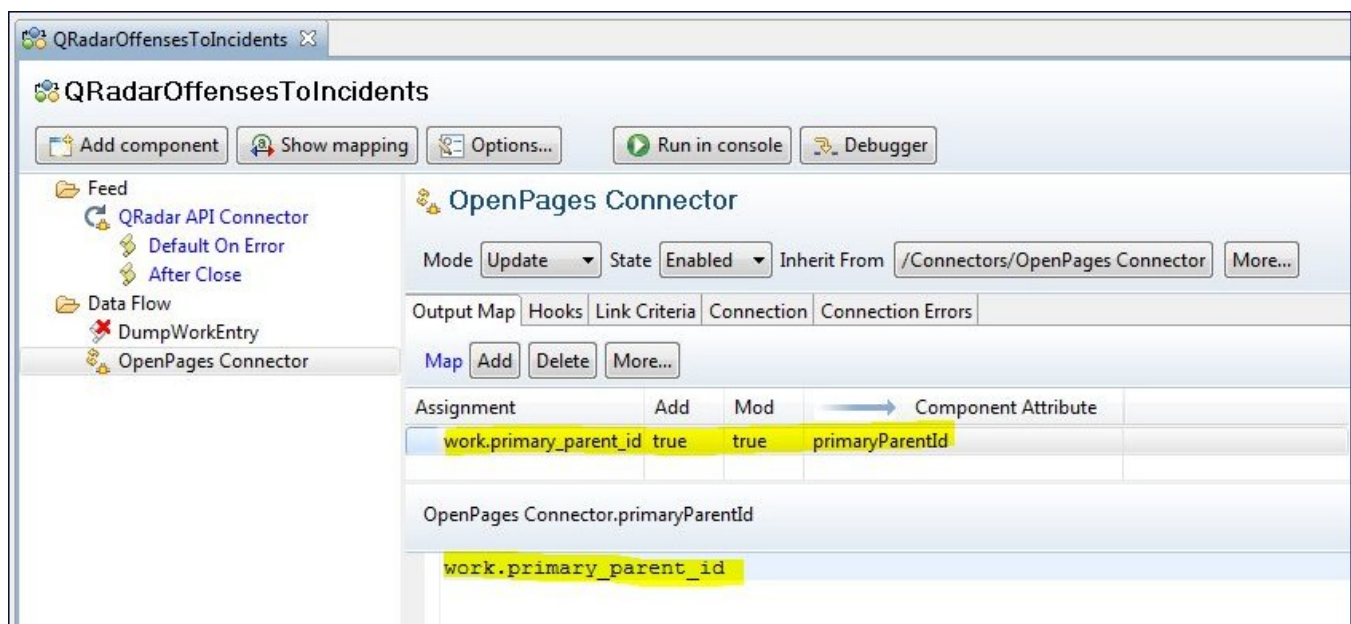


Figure 77. The **work.primary_parent_id** property in the output mapping:

The value must be a number, enclosed in double quotes, and should be the object resource ID of a suitable OpenPages parent object. A null or empty value is ignored. This technique enables the use of a different primary parent ID for each object being created.

- If a **work.primary_parent_id** property value is not supplied in the OpenPages connector output mapping from the preceding technique, then the OpenPages connector looks for non-null values of the following two properties in the output mapping to derive the primary parent ID of a parent object for the new object being created:
 - **work.parent_type**: the OpenPages object type of the parent object
 - **work.parent_location**: the relative location of the OpenPages parent object instance

The following graphic shows the primary parent ID derived from the non-null values of the two properties **work.parent_type** and **work.parent_location** in the output mapping.

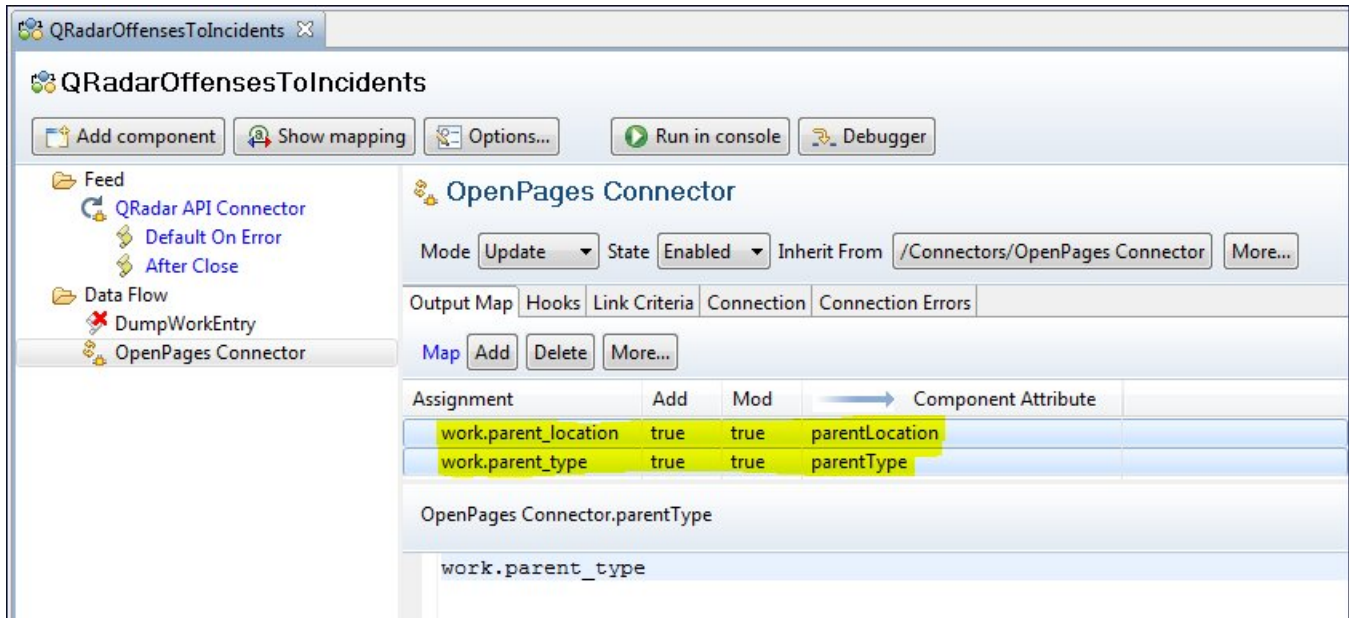


Figure 78. Primary parent ID derived from the non-null values of the two properties **work.parent_type** and **work.parent_location** in the output mapping

See the detailed descriptions and example values provided for the **op_parentType** and **op_parentLocation** properties in the `connector.properties` file, located in the `Runtime-qradar_integration` folder of the SDI `qradar_integration` project. If the values for these properties do not derive to a valid parent object, then they are ignored.

The following graphic shows a detail from the `connector.properties` file:

```

# op_parentType
#
# The GRC object type of the parent object to use for all newly created objects.
#
# Example:    op_parentType=SOXBusEntity
op_parentType=SOXBusEntity

# op_parentLoc
#
# The relative location of the GRC parent object instance to use as the parent for all
# newly created objects. For Business Entity parents, specify all of the segments of the
# Folder location except for the root. For non-Business Entity parents, specify all of
# the segments of the folder location except for the root and append the name of the parent
# object as the last segment of the location. The op_parentLoc property should start with
# a leading '/' character; do not include any spaces around the '/' characters.
#
# Example 1: If a business entity object named 'Audits' has a Folder value of
#   BusinessEntity / Library / Audits
# then specify the relative location, that is, just the segments of the pathname under the
# root folder (in this case the root folder is 'BusinessEntity'), as follows:
#   opParentLoc=/Library/Audits
#
# Example 2: If a business entity object named 'Asia Pacific' has a Folder value of
#   BusinessEntity / Global Financial Services / Asia Pacific
# (where 'BusinessEntity' is the root in the Folder property) then specify the property as:
#   op_parentLoc=/Global Financial Services/Asia Pacific
#
# Example 3: If a non-business entity Risk object named 'Risk1' has a Folder value of
#   Risks/test1
# (where 'Risks' is the root in the Folder property) then specify the property as
# follows, being sure to append the parent object's name (in this example the parent
# object's name is 'Risk1'):
#   op_parentLoc=/test1/Risk1
#
op_parentLoc=/Library/Audits

```

Figure 79. A detail from the *connector.properties* file

This technique enables the use of a different primary parent ID for each object being created.

- If the properties in the preceding two techniques are not provided, then the OpenPages connector uses the default primary parent ID derived from the **op_parentType** and **op_parentLocation** properties defined in the *connector.properties* file, located in the Runtime-qradar_integration folder of the SDI qradar_integration project. The values in the *connector.properties* file are processed once per assembly line execution, and the resulting derived value serves as the default primary parent ID to use if the properties in the two preceding sections are not provided.

If the values for these properties do not derive to a valid parent object, then there will be no default value available for the duration of the assembly line execution. See the detailed descriptions and example values provided for each of these properties in the *connector.properties* file, located in the Runtime-qradar_integration folder of the SDI qradar_integration project.

Specifying currency values to the OpenPages connector by the output mapping

You can specify currency values in the IBM OpenPages with Watson connector output mapping as strings (enclosed with quotation marks) by using a standard format.

About this task

The amount is specified first, followed by a vertical bar, followed by the ISO code. White space is allowed. The entire string must be enclosed in quotation marks.

Procedure

Supply the currency values in the OpenPages connector output mapping as strings, that is, enclosed with quotation marks, by using the following format: "<amount>|<isoCode>"

- Examples of valid currency values in the output mapping: "123.45|AUD" or "321 | USD"
- Example of an invalid currency value in the output mapping because the enclosing quotation marks are missing: 123.45|AUD
- Example of an incomplete currency value in the output mapping because the ISO code is missing; when this situation occurs, the default currency that is configured in OpenPages is used: "123 | "

Specifying date values to the OpenPages connector via the output mapping

Date values should be specified as **java.util.Date** objects in the IBM OpenPages with Watson connector output mapping.

IBM OpenPages SDI Connector for UCF Common Controls Hub integration

You can use IBM OpenPages SDI Connector for UCF Common Controls Hub to bring data from UCF Common Controls Hub into OpenPages. UCF Common Controls Hub is a separate stand-alone web application. It is not included with OpenPages.

UCF is a database of regulatory compliance documents. The regulatory documents are divided into parts, which can then be used by APIs. UCF Common Controls Hub is the web portal to the UCF data.

Data can be pulled from UCF (initiated by IBM Security Directory Integrator), then mapped one-to-one to object types in OpenPages.

Note: IBM Security Directory Integrator is the latest name for IBM Tivoli Directory Integrator.

Table 302. UCF object type mappings	
Object type in UCF	Object type in OpenPages
Authority documents	Mandates
Citations	Sub-Mandates
Controls	Requirements

A mandate can have one or more sub-mandates. A sub-mandate can have zero or more requirements. A requirement can be related to multiple sub-mandates from different mandates.

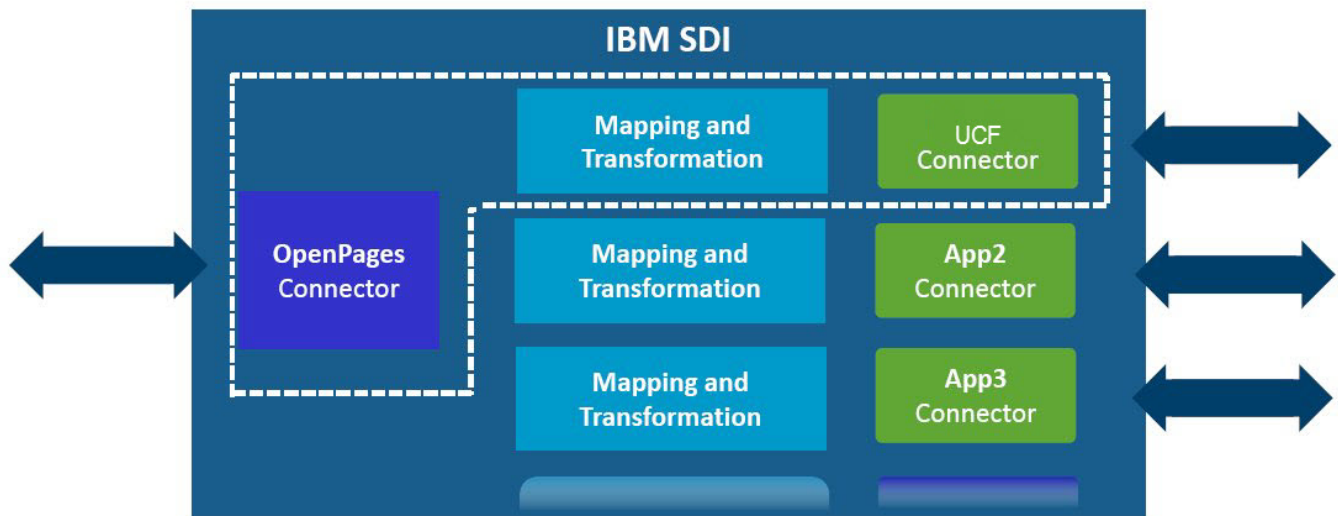


Figure 80. How OpenPages and UCF work together

Run the UCF assembly lines

Run the UCF assembly lines to import objects from UCF Common Controls Hub into OpenPages.

You must install and configure the UCF connector before you begin. For more information, see "Installing UCF integration" in the *IBM OpenPages with Watson Installation and Deployment Guide*.

Run the assembly lines in the following order. Wait for each assembly line to finish before you run the next assembly line:

- UCF Authority Documents to OP Mandates
- UCF Citations to OP Submandates
- UCF Controls to OP Requirements

To run an assembly line, right-click it in the **SDI Configuration Editor** and click **Run AssemblyLine**. To view the log, click .

Note: The UCF connector assembly lines do not support Delta mode.

You can schedule the assembly lines to run by using the IBM Security Directory Integrator scheduler. Set up the scheduler so that each assembly line completes before the next begins.



Attention: The assembly lines will not run when System Admin Mode (SAM) is enabled in OpenPages. The assembly lines write data to the OpenPages database, and System Admin Mode prevents write operations. Ensure that System Admin Mode is disabled before you run the assembly lines. To disable System Admin Mode, click  > **Disable System Admin Mode**.

To view the UCF objects in OpenPages, go to **Compliance > Mandates**. Click **Library > UCF**.

Updating connection information

If you need to update the connection information that the UCF connector uses to connect to OpenPages or to UCF Common Controls Hub, see "Configuring connection information" in the *IBM OpenPages with Watson Installation and Deployment Guide*

Troubleshooting

If an assembly line fails the first time that you run it, open IBM Security Directory Integrator, click the icon to restart the default server, and then run the assembly line again.

If you encounter errors about missing impact zones or guidance areas, update the UCF fields with the new enumerated string values. See "Update business entities and fields" in the *IBM OpenPages with Watson Installation and Deployment Guide*

IBM Security Directory Integrator (SDI) techniques

If you use the IBM OpenPages with Watson connectors, there are SDI techniques that might help you.

Scheduling Security Directory Integrator

IBM Security Directory Integrator (SDI) has a built-in capability for scheduling. Each assembly line can have one or more schedules. SDI can run in a daemon mode between runs, or shut down completely. Assembly lines can also be run on demand by the command line.

In the SDI Configuration Editor, right-click an assembly line and select **Create Schedule**.

If you are using the UCF connector, schedule the assembly lines in the following order. Schedule the assembly lines so that each completes before the next begins.

- UCF Authority Documents to OP Mandates
- UCF Citations to OP Submandates
- UCF Controls to OP Requirements

For more information about scheduling assembly lines, see [IBM Security Directory Integrator Scheduler](#) in the Security Directory Integrator documentation.

Security Directory Integrator command line tips

You can run the assembly lines on your local or remote server where IBM Security Directory Integrator (SDI) is installed.

To run commands on a remote SDI server, you must have SDI installed on your local system. When entering SDI commands on the local server to execute on a remote SDI server, be sure to include the **-h <hostname>** command switch.



Attention:

- If changes are made to any of the properties files that are used by the connector components and you are running SDI as a service, the service must be stopped and restarted for those changes to take effect.
- Logging for SDI running as a service is written to the `ibmdi.log` file in the installed SDI area where the service lives. For example, on a Windows-based system, this is `<SDI-install-root>/win32_service/logs/ibmdi.log` by default.
- When you run an assembly line by using the SDI Configuration Editor, the log entries are put into the `<SDI-solutions-root>/logs/ibmdi.log` by default.

Here are some examples of commands that you can run against your imported configuration. Note the use of the **-h <hostname>** switch when the command is intended to run on a remote SDI server configuration. Also, the use of the **ibmdisrv** command is not typically used, but is included here as an example of how it can be used.

In these examples, the QRadar integration is located inside the SDI workspace at the following location: `C:\SDI_Solutions\workspace\qradar_integration\Runtime-qradar_integration\qradar_integration.xml`.

- `tdisrvctl -v -op start -c C:\SDI_Solutions\workspace\qradar_integration\Runtime-qradar_integration\qradar_integration.xml -r QRadarOffensesToIncidents`
- `tdisrvctl -v -h <hostname> -op start -c C:\SDI_Solutions\workspace\qradar_integration\Runtime-qradar_integration\qradar_integration.xml -r QRadarOffensesToIncidents`

- `ibmdisrv -c "C:\SDI_Solutions\workspace\qradar_integration\Runtime-qradar_integration\qradar_integration.xml" -r "QRadarOffensesToIncidents"`

Troubleshooting the assembly line "Connection refused" error

When you start the IBM Security Directory Integrator (SDI) Configuration Editor, or when you run SDI commands from a command line, you might encounter an error that says the connection to your SDI server is refused.

About this task

This error can be caused by running more than one instance of either the SDI Configuration Editor or the SDI service at the same time on the same server.

Procedure

1. Check for any program that is using port 1099 already by using the following commands:
 - Windows: `netstat -an | findstr 1099`
 - Linux: `netstat -an | grep 1099`
2. If the output of this command is not empty, determine which process is already using port 1099 and stop that process. If the process is already stopped, re-enter the command after a minute or two to ensure that the ports are no longer in use. You might need to repeat the **netstat** command a few times before the output is empty.

Chapter 31. Configuring questionnaire assessments

You can use the questionnaire assessments to assess risk and compliance or to collect information for specific processes and asset risks. This capability streamlines, standardizes, and centralizes the collection of questionnaire-based assessment information.

Configuring questionnaire assessments

To use questionnaire assessments, you set up user permissions for users. You can also configure the email server so that lifecycle triggers send emails to lifecycle assignees. You can customize two visual elements on questionnaire assessments: the logo in the header and the introduction text on the landing page. These elements are displayed on all questionnaire assessments regardless of the questionnaire template and program that is used to create the questionnaire assessments.

Before you begin

Questionnaire assessments move through a review process. The review process can be based either on GRC Workflow or the legacy lifecycle functionality.

If you use lifecycle functionality as a review process, make a plan to transition to GRC Workflow.

If you use GRC Workflow as a review process, determine what questionnaire assessment workflow is used to drive the review process. OpenPages includes an out-of-the-box Questionnaire Assessment Workflow. You can use it as is, modify it to meet your needs, or create your own workflow.

Although workflows replace the legacy lifecycle functionality, lifecycle fields still control behavior in the questionnaire UI. Study the Questionnaire Assessment Workflow. Look at how it sets the following lifecycle fields:

- OPLC-QAssessment:LCStage - sets a stage to Information Gathering, Review, or Approval
- OPLC-Std:LCReadOnly - makes answers read only or not
- OPLC-Std:LCInReview - adds ability to reject or accept answers
- OPLC-QAssessment:LCName - specifies the lifecycle to use

LCStage is a required field. If you create your own workflow, LCStage must be set to Information Gathering for the initial stage. For later stages, setting LCStage is optional.

LCReadOnly and LCInReview fields can be used to render the questionnaire assessment at each stage.

Questionnaire assessments and programs must be assigned a lifecycle in LCName. A lifecycle can be two-stage, three-stage, or four-stage.

If you create your own workflow, set these fields as a questionnaire assessment moves through the workflow stages. Be sure to review who the questionnaire assessment is assigned to at each stage.

The workflow controls the options on both the **Action** button in the Questionnaire Assessment Task View and the **Action** button in the questionnaire UI. The options remain synchronized and the same throughout a workflow. A workflow can be advanced by clicking the button in either the Task View or the questionnaire UI. However, it is a best practice to use the button within the questionnaire UI.

If you use the lifecycle functionality, the lifecycle drives the options on the **Action** button in the questionnaire UI. There is no **Action** button in the Task View.

For more information about GRC Workflow, see [Chapter 15, “Configuring GRC Workflow,”](#) on page 495.

Procedure

1. Configure the email server that is used to route mails to lifecycle assignees. For information see [“Set the mail server address”](#) on page 612.

2. Verify that users who create and launch programs have the following permissions:
 - Read/write/associate access to Questionnaire Template objects.
 - Read/write access to the objects used by Questionnaire Templates: Section Templates, SubSection Templates, and Question Templates.
 - Read/write/associate access to Program objects.
 - Read/write/associate access to Questionnaire Assessment objects.
 - Read/associate access to assets.
 - Lock/unlock permissions on files.
3. Verify that users who complete and review questionnaire assessments have the following permissions:
 - Read access to the objects used by questionnaire templates: Questionnaire Templates, Section Templates, SubSection Templates, and Question Templates.
 - Read access to Program objects. Required for four-stage lifecycle because the program owner is at one point the lifecycle assignee for questionnaire assessments.
 - Read/write/associate access to Questionnaire Assessment objects. You can do this with Record Level Security (RLS), where the current lifecycle assignee has the questionnaire assessment, or with the role template.
 - Read/write/associate/delete access to SOXDocument for attachments.
 - Read access to assets.
4. Customize the logo on the questionnaire assessment to be your company logo. File specifications are as follows:
 - Size: 133 pixels wide by 40 pixels high
 - Type: png
 - Name: logo.png
 - Folder location: ../sosa.war/image/questionnaire/

Changes to the logo file can be overwritten in subsequent upgrades.

Copy the file to the folder location. No further setup is necessary. If you do not customize the logo, the system displays the product name in the header rather than a logo.
5. Customize the introduction text that is displayed on the landing page when a respondent opens a questionnaire assessment.
 - a) Go to  > **System Configuration** > **Application Text**.
Or, in the Standard UI, **Administration** > **Application Text**.
 - b) Click **Labels**.
 - c) Write the text and save it in questionnaire.intro.label.informationDetails.

Chapter 32. Configuring timesheet helpers for auditors

The IBM OpenPages Internal Audit Management solution includes helpers for timesheet entry and approval. The helpers also include reports to help with audit planning and management.

There are two timesheet helpers:

- **Timesheet Entry Helper:** This helper enables you to enter time and expenses.

If you have the appropriate permissions, you can also use the Timesheet Entry Helper to enter time on behalf of another auditor.

You can configure the helper by using the settings under **Solutions > IAM > Timesheet Entry > Timesheet Entry Helper**.

- **Timesheet Approval Helper:** This helper enables you to review and approve time and expenses.

You can configure the Timesheet Approval Helper by using the settings under **Solutions > IAM > Timesheet Entry > Timesheet Approval Helper**.

For more information about the IBM OpenPages Internal Audit Management solution and the timesheet helpers, see the *IBM OpenPages with Watson Solutions Guide*.

Chapter 33. Configuring the approval app

The approval app is an optional feature that leverages the power of IBM OpenPages with Watson and provides an easy-to-use interface for quickly taking action on a review, approval, or attestation request with confidence and full knowledge of the context surrounding the request. The approval app works with objects that are set up for the configurable lifecycle.

By using the approval app, a casual or infrequent user of IBM OpenPages with Watson is now able to make well-informed decisions for GRC tasks guided by information from the system quickly and easily, without the need for extensive training in OpenPages. If you want to see all of the items sent to you in the approval app, you can go to your To Do list by clicking the IBM OpenPages with Watson logo. You simply make the decision (or respond to certification language or questions), with your comments if necessary, and click the relevant button to submit. You can use this feature on tablets and mobile devices as well, for increased flexibility.

Configuring the JSON file for the approval app

You use the `deck_config.json` file as a place to configure object types, fields, and so on, for the approval app.

About this task

The `deck_config.json` is preconfigured to be ready for use. If you want, there are other changes that you can make. For more information, see [“Customizing the JSON file for the approval app” on page 1001](#).

The following table contains the property list and instructions for the `deck_config.json` file properties.

Table 303. Properties in <code>deck_config.json</code>				
Property	Needed	Parent Property	Description	Value (example)
profile	exactly 1	root property	Name of the OpenPages profile used by the approval app	approval app
objectTypes	1 to many	root property	List of the approval app supported object types (system names)	SOXControl
objects	1 per objectType	root property	List of properties for each object type	[{}]
type	1	objects	Type of the OpenPages object system name	SOXControl
fieldTitle	1	objects	Field to be used as the name of the object	Name
fieldDesc	1	objects	Field to be used as the description of the object	Description
lifecycle	1	objects	List of lifecycle properties for object	{}
enabled	1	lifecycle	Boolean to enable object for the approval app	true

Table 303. Properties in *deck_config.json* (continued)

Property	Needed	Parent Property	Description	Value (example)
stageMap	1	lifecycle	List of the approval app enabled lifecycle stages	{}
"Attestation"	1 to many	stageMap	List of properties for the approval app enabled lifecycle stage	{}
showInList	1	"Attestation"	Boolean to display stage in the approval app	true
questionFieldLists	1	"Attestation"	List of question field properties for certification	[{}]
rule	1 to many	questionFieldLists	Rule to determine whether a question is used	default
fields	1 per rule	questionFieldLists	List of question fields for certification	[{}]
systemName	1 to many	fields	OpenPages system name of certification question field	OPSS-Ctl-Cert:DesEff
displayType	1 per systemName	fields	the approval app-specific display type for the certification field	Text Area
widgetList	1	objects	List of properties for the controlling views in OpenPages	[{}]
attachmentList	0 or 1	widgetList	Controls the display of the Files list under the Related Content section in the approval app. • show: Always display the Files list. • hide: Always hide the Files list. If you want to show files or links, you must add them to the profile view of the object. • auto: Shows the Files list. But if the profile view includes files or links, hides the Files list. Default: auto	show

Table 303. Properties in `deck_config.json` (continued)

Property	Needed	Parent Property	Description	Value (example)
name	1	widgetList	Name of the approval app section controlled by a view	details
type	1	widgetList	Type of the OpenPages view controlling the approval app section	ActivityView
activityView	1	widgetList	Name of the OpenPages view controlling the approval app section	OP-Deck-Control
parentViews	0 to 1	widgetList	List of OpenPages views displayed in the approval app Related Content section	[{}]
type	1 to many	parentViews	Type of the OpenPages parent object system name	SOXRisk
activityView	1 per type	parentViews	Name of the OpenPages view controlling the approval app section	OP-Deck-LE-Risk
dueDateGroup	1	root property	List of properties for grouping the items in the approval app	{}
defaultField	1	dueDateGroup	Field to be used as the Due Date field	OPLC-Std:LCDDueDate
group	0 to 1	defaultField	List of properties controlling the date ranges for grouping in the approval app	[{}]
number	1 to many	group	Date range for grouped items	14
unit	1 per number	group	Unit of measurement for group date range (day, month, or year)	day
maxTodoObjects	1	root property	Number of items to be displayed in the approval app	25

Debugging the `deck_config.json` file

You can debug the `deck_config.json` file by logging into OpenPages as an administrator and pasting a URL (`http://<yourIP>:<port>/openpages/app/deck/reloadConfig`) in the browser. If there is an error in the `deck_config.json` file, a message displays that shows details about the error, such as the error number, exception type, line number, and error description. The error is logged in the aurora log as well. You can then locate and fix the error in the `deck_config.json` file.

To perform this procedure, you must have the **OpenPages Platform 3** profile associated with your user name.

Procedure

1. Click  > **System Configuration** > **System Files**.
2. Expand the End User Applications Config folder to find the deck_config.json file.
3. Configure the deck_config.json file according to the preceding table.

The following example shows a typical deck_config.json file.

```
{
  "profile": "Deck",
  "objectTypes" : ["SOXControl", "SOXIssue", "LossEvent", "Incident"],
  "objects" : [
    {
      "type" : "SOXControl",
      "fieldTitle" : "Name",
      "fieldDesc" : "Description",
      "lifecycle" : {
        "enabled" : true,
        "stageMap" : {
          "Attestation" : {
            "showInList": true,
            "questionFieldLists" : [
              {
                "rule" : "default",
                "fields" : [{
                  "systemName": "OPSS-Ctl-Cert:DesEff",
                  "displayType": "Radio Button/Checkbox"
                },
                {
                  "systemName": "OPSS-Ctl-Cert:DesEffExplain",
                  "displayType": "Text Area"
                },
                {
                  "systemName": "OPSS-Ctl-Cert:DocAccurate",
                  "displayType": "Radio Button/Checkbox"
                },
                {
                  "systemName": "OPSS-Ctl-Cert:DocAccurateExplain",
                  "displayType": "Text Area"
                },
                {
                  "systemName": "OPSS-Ctl-Cert:OpEff",
                  "displayType": "Radio Button/Checkbox"
                },
                {
                  "systemName": "OPSS-Ctl-Cert:OpEffExplain",
                  "displayType": "Text Area"
                },
                {
                  "systemName": "OPSS-Ctl-Cert:Change",
                  "displayType": "Radio Button/Checkbox"
                },
                {
                  "systemName": "OPSS-Ctl-Cert:ChangeExplain",
                  "displayType": "Text Area"
                }
              ]
            }
          }
        }
      }
    },
    {
      "name" : "details",
      "type" : "activityView",
      "activityView" : "OP-Deck-Control",
      "parentViews" : [
        {
          "type" : "SOXRisk",
          "activityView" : "OP-Deck-Control-Risk"
        }
      ]
    }
  ],
  "widgetList" : [
    {
      "type" : "SOXIssue",
      "fieldTitle" : "Name",
```



```

        "fieldDesc" : "Description",
        "lifecycle" : {
            "enabled" : true,
            "stageMap" : {
                "Close Request" : {"showInList": true},
                "Due Date Change Request" : {"showInList": true}
            }
        },
        "widgetList" : [
            {
                "name" : "details",
                "type" : "activityView",
                "activityView" : "OP-Deck-Issue"
            }
        ]
    },
    {
        "type" : "LossEvent",
        "fieldTitle" : "Name",
        "fieldDesc" : "Description",
        "lifecycle" : {
            "enabled" : true,
            "stageMap" : {
                "Awaiting Approval" : {"showInList": true},
                "Awaiting Approval L1" : {"showInList": true},
                "Awaiting Approval L2" : {"showInList": true}
            }
        },
        "widgetList" : [
            {
                "name" : "details",
                "type" : "activityView",
                "activityView" : "OP-Deck-LE",
                "parentViews" : [
                    {
                        "type" : "SOXRisk",
                        "activityView" : "OP-Deck-LE-Risk"
                    }
                ]
            }
        ]
    },
    {
        "type" : "Incident",
        "fieldTitle" : "Name",
        "fieldDesc" : "Description",
        "widgetList" : [
            {
                "name" : "details",
                "type" : "activityView",
                "activityView" : "OP-Deck-Incident"
            }
        ],
        "lifecycle" : {
            "stageMap" : {
                "Review" : {"showInList": true},
                "Escalation Review" : {"showInList": true}
            }
        }
    }
],
"dueDateGroup" : {
    "group" : [{"number": 5, "unit": "day"}, {"number": 30, "unit": "day"}]
},
"maxTodoObjects" : 25
}

```

Approval app certification questions

Approval app certification questions provide an opportunity to prompt a user taking a lifecycle action to respond to questions that certify the details of what they are agreeing to. Certification questions can also remind them of the requirements of the certification or attestation they are performing.

The following table shows the supported field data types:

Field data type	Supported	Details	Valid deck_config.json displayType value
Currency	X		
Enumerated String	X	Single-select only	Radio Button/Checkbox
Simple String	X		Text and Text Area
Long String	X	Medium String Size only	Text and Text Area



Attention:

- Certification questions display the field guidance as the Question in the approval app—not as the field label, as the field guidance does in OpenPages.
- For the approval app, if a field-level security (FLS) rule is applied on a question, the question is still displayed on the card page for the lifecycle stage that is configured in the deck_config.json file, even if the user does not meet the FLS rule to view the question. When the user submits the question, the user sees the following message: You do not have permission to write on the field <field name>.

The following list shows some example certification questions.

Certification Language without values

Use a single-select Enumerated String field. This causes the question to appear without any values to select.

Single select checkbox

Use a single-select Enumerated String field with a single value. This causes the question to appear with a single check box.

Make a follow up question required

Use Requiredness field dependencies in OpenPages.

Note: The approval app does not support both Requiredness and Visibility dependencies at the same time.

Hide a follow up question unless a specific Enum value is selected

Use Visibility field dependencies in OpenPages.

Note: The approval app does not support both Requiredness and Visibility dependencies at the same time.

For a transition, make the lifecycle comment or other Simple/Long string required

```
"<SOME_STAGE>" : {
  "transitionMap" : {
    "<SOME_TRANSITION>" : {
      "requiresValidation" : true
    }
  },
  "questionFieldLists" : [
    {
      "rule" : "default",
      "fields" : [{
        "systemName": "<COMMENT/OTHER FIELD NAME>",
        "displayType": "Text Area",
        "requiredValue" : "NON_EMPTY"
      }]
    }
  ]
}
```

Make a Simple/Long string field appear in a single-line text box

```
"<SOME_STAGE>" : {
  "questionFieldLists" : [
    {
      "rule" : "default",
```

```

    "fields" : [{
      "systemName": "<FIELD NAME>",
      "displayType": "Text"
    }]
  }
]
}

```

Make a Simple/Long string field appear in a multi-line text area

```

"<SOME_STAGE>" : {
  "questionFieldLists" : [
    {
      "rule" : "default",
      "fields" : [{
        "systemName": "<FIELD NAME>",
        "displayType": "Text Area"
      }]
    }
  ]
}

```

Customizing the JSON file for the approval app

The `deck_config.json` file is ready to use, but you can customize it.

About this task

The `deck_config.json` is preconfigured to be ready for use. If you want, there are changes that you can make. For example, the `parentViews` property is optional: its default value is 0, in which case no parent objects are shown even though the `parentViews` property supports multiple parent views.

This configuration example shows how to define what appears in the Related Content section for the Controller object.

```

"parentViews" : [
  {
    "type" : "SOXBusEntity",
    "activityView" : "OP-Deck-Control-BE"
  },
  {
    "type" : "SOXRisk",
    "activityView" : "OP-Deck-Control-Risk"
  }
]

```

The following examples show various cases of properties that are supported but might not be enabled by default.

Example: Grouping a To Do list for 5 and 30 days

```

"dueDateGroup" : {
  "group" : [{"number": 5, "unit": "day"}, {"number": 30, "unit": "day"}]
}

```

Example: Making the comment field a required field for specified transitions

The comments field is not required in the standard configuration, and users can transition in a detail page without adding a comment.

You might submit an action in the approval app and see a message similar to the following: Success! Your <action> and comments have been submitted to <recipient>, even though there are no comments.

You can configure the comment field to be a required field for specified transitions in the `deck_config.json` file. In the following case, the comment field is required for the Review De-escalate transition of the Escalation Review lifecycle stage.

```

      "Escalation Review" : {
        "transitionMap" : {
          "Review De-escalate" : {
            "requiresValidation" : true

```

```

    },
    "questionFieldLists" : [
    {
      "rule" : "default",
      "fields" : [{
        "systemName": "OPLC-Std:LCCComment",
        "displayType": "Text Area",
        "requiredValue" : "NON_EMPTY"
      }]
    },
    {
      "rule" : "default",
      "fields" : [{
        "systemName": "DECK-Questions:EnumQuestion",
        "displayType": "Radio Button/Checkbox"
      }]
    }
  ]
}

```

Example: Approval app stage with certification questions

```

"stageMap" : {
  "Attestation" : {
    "showInList": true,
    "questionFieldLists" : [
      {
        "rule" : "default",
        "fields" : [{
          "systemName": "OPSS-Ctl-Cert:DesEff",
          "displayType": "Radio Button/Checkbox"
        },
        {
          "systemName": "OPSS-Ctl-Cert:DesEffExplain",
          "displayType": "Text Area"
        }
      ]
    ]
  }
}

```

Chapter 34. Configuring OpenPages Loss Event Entry

IBM OpenPages Loss Event Entry is an optional, chargeable component that users across an organization can access to create loss events. You can customize the component by configuring how it works for your organization, and the way users view and interact with it. OpenPages Loss Event Entry can be used to create only loss events together with loss impacts, loss recoveries, and files. You cannot use it to create other object types.

You use the Loss Event Entry Configuration tool to configure the OpenPages Loss Event Entry component. For more information about this tool, see [“Using the Loss Event Entry Configuration tool”](#) on page 1010. Review that topic and access and open the tool as you learn about how to configure OpenPages Loss Event Entry.

Read [“Planning the configuration”](#) on page 1003 to learn about whether you can use the out-of-the-box configuration that is included in OpenPages Loss Event Entry. If you choose to modify the out-of-the-box configuration, the following topics explain aspects of the system you need to understand before you begin:

- [“How users are handled”](#) on page 1005
- [“Where loss events get created”](#) on page 1005
- [“Who loss events get assigned to”](#) on page 1005
- [“How dates are validated”](#) on page 1006
- [“How to launch OpenPages Loss Event Entry”](#) on page 1006
- [“How confirmation emails are configured”](#) on page 1009

For more information about OpenPages Loss Event Entry, see the topic *OpenPages Loss Event Entry* in the *IBM OpenPages with Watson New Features Guide*.

Planning the configuration

You can use OpenPages Loss Event Entry either as it is out-of-the-box with a minimal amount of configuration or you can make modifications for your organization.

To use OpenPages Loss Event Entry as it is out-of-the-box, you need to complete the following configuration tasks:

1. In the Loss Event Entry Configuration tool, change the passwords of the ten dedicated users that are included in OpenPages Loss Event Entry. For information, see [“Using the Loss Event Entry Configuration tool”](#) on page 1010.
2. Review the creation views for loss events and decide whether you want to display or hide the **Loss Impacts** and **Loss Recoveries** tabs. If displayed, you can also decide whether to make them mandatory. Creation views are described later in this topic. How you can make the tabs mandatory is described in [“Using the Loss Event Entry Configuration tool”](#) on page 1010.
3. Change the role template assignment for the Loss Event Entry role template so that it grants the lowest level of access needed.
4. In the Loss Event Entry Configuration tool, define **Default Parent Path** and **Default Triage Team**. For information, see [“Using the Loss Event Entry Configuration tool”](#) on page 1010.
5. Place a URL on your organization's intranet. For information, see [“How to launch OpenPages Loss Event Entry”](#) on page 1006.

You can, alternatively, modify many aspects of OpenPages Loss Event Entry. To do this, review what is included in the system and modify any of the following items to meet your requirements:

- Decide what locales you need. It is a best practice to disable locales that you do not use and disable or do not load the dedicated users for them.

- Review the user group, Loss Event Entry, and make changes if needed. It contains ten dedicated users, one for each locale: LEE_EN_US, LEE_EN_GB, LEE_IT_IT, LEE_PT_BR, LEE_FR_FR, LEE_ES_ES, LEE_DE_DE, LEE_ZH_TW, LEE_ZH_CN, and LEE_JA_JP. For more information, see [“How users are handled”](#) on page 1005.
- Review the role template, Loss Event Entry, and make changes if needed. The ten dedicated users are assigned to this role template at the root business entity. It is a best practice to change the role template assignment for the Loss Event Entry role template so that it grants the lowest level of access needed.
- Review the profile, Loss Event Entry, and make changes if needed. The ten dedicated users are assigned to this profile.
- Design the content of the loss event form. Review the creation views, LE Entry - LE, LE Entry - LI, and LE Entry - LR, and make changes if needed. They are assigned to the Loss Event Entry profile. The system uses the views to determine what tabs and fields are displayed in OpenPages Loss Event Entry. Decide whether you want to display or hide the **Loss Impacts** and **Loss Recoveries** tabs. Both tabs are set to display in the creation views included with the system. To hide them, remove them as child views on LE Entry - LE. If you want to display these tabs in creation views you create, they must be defined as child views on the loss event creation view. If you want to make it mandatory that a user enter a loss impact or loss recovery, you can configure that in the Loss Event Entry Configuration tool.
- Review the field groups, OPSS-LE-BE and OPSS-LE-Contact. OPSS-LE-BE contains Business Entity Selector fields that are used to identify the involvement of business entities in loss events. OPSS-LE-Contact contains fields that contain user information such as name, email, and phone number.
- Review the date validation rules that are included in the system and make changes if needed. You configure date validation rules in the Loss Event Entry Configuration tool. For information, see [“How dates are validated”](#) on page 1006.
- Determine how you want to set the parent business entity and the triage team. For information, see [“Where loss events get created”](#) on page 1005 and [“Who loss events get assigned to”](#) on page 1005. Fields that contain parent business entities must be of the display type, Business Entity Selector. For information about this display type, see [“Configuring the Business Entity Selector display type for simple string fields \(Standard UI\)”](#) on page 350.
- Enable auto-naming for the Loss Event, Loss Impact, and Loss Recovery objects. Although not required, it prevents failures due to duplicate names and inconsistencies in user-given names. Users who create loss events do not know the naming rules in OpenPages.
- Customize the informational text displayed in OpenPages Loss Event Entry.
 - To change the text that displays when users click the  icon for the Information box in the header, change the text associated with the Application Text key, loss.event.entry.overall.help, in the Application Messages folder.
 - To change the information that is displayed at the top of the tab for each object type, change the text for the keys, loss.event.entry.file.intro, loss.event.entry.loss.event.intro, loss.event.entry.loss.impact.intro, and loss.event.entry.loss.recovery.intro in the Application Messages folder.
 - Customize the logo on the loss event form to be your company logo. File specifications are as follows:
 - Size: 1130 pixels wide by 36 pixels high
 - Name: Logo.png
 - Folder location: ../sosa.war/image/lossevent/
 Changes to the logo file can be overwritten in subsequent upgrades.
- Design and configure the email confirmation that is sent to users when a loss event is created. For information, see [“How confirmation emails are configured”](#) on page 1009.

How users are handled

Users can create loss events in OpenPages Loss Event Entry without a user account for OpenPages. A dedicated user group that includes ten dedicated users, one for each supported locale, is included in OpenPages Loss Event Entry. When users access OpenPages Loss Event Entry, they do not have to enter a user ID and password. The system automatically logs them in to OpenPages Loss Event Entry with the dedicated user associated with the locale.

Users with access to OpenPages can create loss events as they always have or choose to use OpenPages Loss Event Entry. However, OpenPages users cannot log in to both at the same time in the same browser. Instruct your OpenPages users that they must log out of OpenPages when they want to use OpenPages Loss Event Entry. If you want to force OpenPages users to use IBM OpenPages Loss Event Entry, you can add Loss Event to the list of objects that are disabled for Add New. For more information, see [“Controlling the availability of object types in the Add New wizard” on page 286](#). Additionally, the profile and role template assignments for OpenPages users is disregarded when they use OpenPages Loss Event Entry.

Where loss events get created

Loss events must be assigned to a parent business entity within the organization. You determine how this assignment is made when you define Default Parent Path and Parent Field Name in the Loss Event Entry Configuration tool.

For information about the Loss Event Entry Configuration tool, see [“Using the Loss Event Entry Configuration tool” on page 1010](#).

You can choose one of the following methods:

- Static: your organization assigns all loss events to one default business entity. The triage team then reassigns them to the correct business entities. To use this method, you enter the default business entity in **Default Parent Path** and leave **Parent Field Name** blank.
- User-selected: your organization assigns loss events to a business entity that the user selects, for example, the Primary Caused Entity or the Primary Impacted Entity. To use this method, you enter the field name that contains the business entity in **Parent Field Name**. The field must be in the creation view.
- Pre-filled in a URL: your organization assigns loss events to a business entity that you pass in the URL. To use this method, you enter the field name that contains the business entity in **Parent Field Name**. Pass the value that you want in the URL.
- Custom: your organization sets the business entity based on information in the loss event or elsewhere in the system. For example, the system can automatically assign a loss event to Business Entity A if the loss amount is less than \$1,000,000 and to Business Entity B if it is over that amount. This method can be implemented with triggers. To use this method, you can leave **Parent Field Name** blank because it is set by the triggers.

The **Default Parent Path** is mandatory for all methods. The system defaults to it if the value in **Parent Field Name** is not given, is invalid, or there is an error. Ensure that the dedicated users have access rights to create loss events under the business entity in **Default Parent Path**.

Who loss events get assigned to

Loss events are typically assigned to a triage team that is responsible for reviewing the initial information and taking next steps. You determine how this assignment is made when you define **Default Triage Team** and **Triage Team Field Name** in the Loss Event Entry Configuration tool.

For information about the Loss Event Entry Configuration tool, see [“Using the Loss Event Entry Configuration tool” on page 1010](#).

You can choose one of the following methods:

- **Static:** your organization assigns all loss events to a list of users and user groups. To use this method, you enter the list of users and user groups in **Default Triage Team** and leave **Triage Team Field Name** blank.
- **User-selected:** your organization assigns loss events to users or user groups that the user selects. To use this method, you put the field name that contains the actor field in **Triage Team Field Name**. The field must be in the creation view.
- **Pre-filled in a URL:** your organization assigns loss events to users or user groups that you pass in the URL. To use this method, you put the field name that contains the actor field in **Triage Team Field Name**.
- **Custom:** your organization assigns loss events to user or user groups based on information in the loss event or elsewhere in the system. For example, a trigger can take the value of a loss event's Primary Impacted Entity field and go to that entity's Preference record to get the name of the triage team. It can then put that triage team name into the triage team field on the loss event. To use this method, you can leave **Triage Team Field Name** blank because it is set by the triggers.

The **Default Triage Team** is mandatory for all methods. The system defaults to it if the value in **Triage Team Field Name** is not given, is invalid, or there is an error. Ensure that the field given in **Triage Team Field Name** is one of the seven actor display types. If you pre-fill it in a URL, ensure that the values passed in the URL are consistent with the actor display types you chose in the **Triage Team Field Name**.

A third field, **Populate Triage Team Field Name**, is typically used as the assignee in the first stage in configurable life cycles for loss events. It is a mandatory field. When a loss event is created, the users and user groups in **Triage Team Field Name** are copied to the field given in **Populate Triage Team Field Name**. If **Triage Team Field Name** is not given, the users and user groups in **Default Triage Team** are copied to the field given in **Populate Triage Team Field Name**. All three field types must be compatible. The display type of the field that is given in **Populate Triage Team Field Name** must be able to accept any value that comes from **Default Triage Team** or **Triage Team Field Name**. For example, if **Triage Team Field Name** is a multiple user/group field, **Populate Triage Team Field Name** must also be a multiple user/group field.

How dates are validated

You define how dates are validated in rules in the **Date Validation** field in the Loss Event Entry Configuration tool. For example, you might want to ensure that a loss event's discovery date occurs before today's date or that its discovery date falls after its occurrence date.

The following date validation rules would test for these situations:

```
LossEvent:0PSS-LossEV:Discovery Date >= LossEvent:0PSS.LossEV:Occurrence Date
```

```
LossEvent:0PSS-LossEV:Discovery Date <= TODAY
```

OpenPages Loss Event Entry displays a red X and an explanation next to dates that fail the validation rules. Users must resolve errors before they can submit a loss event.

OpenPages Loss Event Entry includes date validation rules that you can keep or modify. The date validation rules are effective only in OpenPages Loss Event Entry and not in OpenPages. If you want the same rules to apply in OpenPages, they can be implemented with triggers.

How to launch OpenPages Loss Event Entry

Users typically access IBM OpenPages Loss Event Entry from one or more links on your organization's intranet.

There are many ways that you can configure the URLs in these links:

- You do not pass parameters in the URL. Use this approach if you want users to provide information for loss events and you do not want to pre-fill information for them.

- You can set what locales users access. If all users access one locale, you can add the locale to the URL in the link on your organization's intranet. If users can access multiple locales, you can either place multiple links on your organizations intranet, for example, a link for users in North America and a link for users in France, or you can have one link and pre-fill the locale in the URL.
- You can pre-fill user information on the loss event form by passing fields and values in the URL. You can include user data from the network login and determine programmatically how to put it in the URL. When a user creates a loss event, values from the URL can pre-fill fields on the form. For example, the user's name, phone number, and email can be passed in the URL so that the user does not have to enter this information.
- You can pre-fill where in the organizational structure the loss event will be created and who it will be assigned to. Use this approach if your organization is structured in a way that loss events can be created in and assigned to multiple areas of the organization. You can use multiple URLs to pre-fill the primary caused business entity and the triage team. Then, users who create loss events do not have to enter this information, it is pre-filled for them and set to the correct value for where they are in the organization.
- You can pre-fill no information so that users can create loss events anonymously. Create a link where you do not pass user information. You must also ensure that users are not required to provide their name and email on the loss event form.

Follow these guidelines when you construct a URL:

- The fields that you pass must be defined for the top-level Loss Event object type.
- The fields that you pass must exist in the creation view.
- The fields that you pass cannot be read-only.
- The fields that you pass must be defined as simple string fields. Other fields types are not supported.
- The display type of the simple string fields that you pass can be: Text Box, Text Area, URL, Business Entity Selector, User Drop-down, User Selector, Group Selector, User/Group Selector, Multi-Valued User Selector, Multi-Valued Group Selector, and Multi-Valued User/Group Selector. All other display types are not supported.
- The values that you pass must be valid for the display type.
- The URL is limited to 2083 characters for Microsoft browsers.

Follow these syntax rules when you construct a URL:

- Start the first parameter with ?.
- Separate multiple parameters with &.
- Provide locales in the format `locale=<locale code>`. Valid locale codes are:
 - `en_US` (US English)
 - `en_GB` (UK English)
 - `it_IT` (Italian)
 - `pt_BR` (Brazilian Portuguese)
 - `fr_FR` (French)
 - `es_ES` (Spanish)
 - `de_DE` (German)
 - `zh_TW` (Chinese Traditional)
 - `zh_CN` (Chinese Simplified)
- Provide fields and values in the format `<field group>:<field name>=<field value>`. Enter the field name not the field label.
- For fields whose display type is Multi-Valued User Selector, Multi-Valued Group Selector, or Multi-Valued User/Group Selector, you can pre-fill the field with one or multiple values. Begin and end values with \$;, for example:

```
$;user1$;
```

Separate multiple values with \$; , for example:

```
$;user1$;user2$;user3$;
```

- For text fields that pass email addresses, for example, **Submitter Email Field Name**, you can pre-fill the field with only one value.

The following examples illustrate how you can construct URLs.

Example 1: Set the locale.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent?locale=en_GB
```

Example 2: Pre-fill the primary caused entity to /Global Services/North America Banking. The display type of OPSS-LE-BE:Primary Caused Entity is business entity selector.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent  
?OPSS-LE-BE:Primary Caused Entity=/Global Services/North America Banking
```

Example 3: Pre-fill the triage team to Risk Team New York and two users:

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent  
?ABC-LE:UsersToNotify=$;Risk Team New York$;user1$;user2$;
```

Example 4: Pre-fill user information from the network sign-on:

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent  
?OPSS-LE-Contact:Your Name=User One&OPSS-LE-Contact:Your Email=user1@example.com
```

Example 5: Pre-fill user information, primary caused business entity, and locale:

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent  
?OPSS-LE-Contact:Your Name=User One&OPSS-LE-Contact:Your Email=user1@example.com  
&OPSS-LE-Contact:Your Phone=555-111-2222&OPSS-LE-BE:Primary Caused Entity=  
/Global Services/North America Banking&locale=en_GB
```

Example 6: Pre-fill information if you have multiple primary caused business entities and multiple triage teams in your organization. Assume that you have two divisions, /Global Services/North America/Division/East and /Global Services/North America/Division/West. You want to prefill the parent business entity with the division's Primary Caused Entity and the triage teams from ABC-LE:UsersToNotify.

You create two URLs. This URL is for users in the East division.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent  
?OPSS-LE-BE:Primary Caused Entity=/Global Services/North America/Division/East  
&ABC-LE:UsersToNotify=DivisionEastTriage
```

This URL is for users in the West division.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent  
?OPSS-LE-BE:Primary Caused Entity=/Global Services/North America/Division/West  
&ABC-LE:UsersToNotify=DivisionWestTriage
```

Example 7: Pre-fill no information for a URL that you use for loss events that are created anonymously. Do not pass user information. You might want to send the email confirmation to a person designated to handle these situations.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent  
?LE-Submitter:Confirmation Emails=user5@example.com
```

Note: You cannot use IBM OpenPages Loss Event Entry and IBM OpenPages with Watson at the same time. To return to OpenPages, close the IBM OpenPages Loss Event Entry browser window, open a new browser window, and then log in to OpenPages.

How confirmation emails are configured

You can design and configure the confirmation email that is sent to users when a loss event is created.

The confirmation email has the following parts:

- Submitter email address

Define **Submitter Email Field Name** in the Loss Event Entry Configuration tool. Email confirmations are sent to this email field. The default is `OPSS-LE-Contact:Your Email`.

- Text and parameters to put in the subject

To build the email subject, you define fields in **Submitter Email Subject Parameters** in the Loss Event Entry Configuration tool that you want to put in the email subject. Then, write the text and enter parameters for those fields in `lossevent.confirm.subject` Application Text. The order of the fields that are listed in **Submitter Email Subject Parameters** must match the numbering of the parameters in the `lossevent.confirm.subject` Application Text.

- Text and parameters to put in the body text

To build the email body text, you define fields in **Submitter Email Body Parameters** in the Loss Event Entry Configuration tool that you want to put in the email body text. Then, write the text and enter parameters for those fields in `lossevent.confirm.content` Application Text. The order of the fields that are listed in **Submitter Email Body Parameters** must match the numbering of the parameters in the `lossevent.confirm.content` Application Text.

- Sender email address

Enter the system email address that sends confirmation emails in `lossevent.confirm.from.address` Application Text. Parameters are not allowed in `lossevent.confirm.from.address`.

Use the following syntax in `lossevent.confirm.subject` Application Text:

- Enter `{0}` for the first parameter, which in the out-of-the box configuration is the name of the loss event. Enter remaining parameters in the syntax `{value}`. The values of fields given in **Submitter Email Subject Parameters** are put in the email subject.

Use the following syntax in `lossevent.confirm.content` Application Text:

- Enter `{1}` for the first parameter, which in the out-of-the box configuration is the name of the submitter. Enter remaining parameters in the syntax `{label}:{value}` or `{value}`. For example, `{2}:{3}` puts the label and value of the second field given in **Submitter Email Body Parameters** in the email body. Then, `{4}:{5}` puts the third field, `{6}:{7}` the fourth field, and so on. For example, `{2}:{3} \n {4}:{5}` puts the second field's label and value, a line break, and the third field's label and value in the body text. Enter `{value}` to omit a field label. For example, `{3} \n {5}` puts the second field's value, a line break, and the third field's value in the body text (without the field labels).
- Use `$children` to include loss event impacts and loss recoveries in the email.
- Use `$title` to include the label of the loss event object type in the email.
- Enter `\n` to force a line break.

For example, if **Submitter Email Body Parameters** is defined as:

```
OPSS-LE-Contact:Your Name,OPSS-LossEv:Owner,System Fields:Name,  
System Fields:Description,OPSS-LE-BE:Primary Caused Entity
```

And `lossevent.confirm.content` Application Text is defined as:

```
{1}, \nThe following $title was entered by you. \n{2}: {3} \n{4}: {5} \n{6}: {7}\n \n  
{8}: {9} \n $children  
\n\nIf you are an OpenPages user, you can click $url to view in OpenPages.  
\n\nDo not reply. Automated email from OpenPages
```

The confirmation email contains the following body text:

```
User One,  
The following Loss Event was entered by you.  
Owner: $;user1$;OpenPagesAdministrator$;  
Name: Library_LE_0022  
Description: This is a description  
Primary Caused Entity: /Global Services/North America  
  
Do not reply. Automated email from OpenPages
```

The value for OPSS-LE-Contact:Your Name is substituted into parameter {1} followed by a line break, text, and another line break.

The label and value for OPSS-LossEv:Owner is substituted into parameters n{2}: {3} followed by a line break.

The label and value for System Fields:Name is substituted into parameters n{4}: {5} followed by a line break.

The label and value for System Fields:Description is substituted into parameters n{6}: {7} followed by a line break.

The label and value OPSS-LE-BE:Primary Caused Entity is substituted into parameters n{8}: {9} followed by a line break.

The ending text is included.

Using the Loss Event Entry Configuration tool

You use the Loss Event Configuration tool to configure IBM OpenPages Loss Event Entry.

Before you begin

Read Chapter 34, “Configuring OpenPages Loss Event Entry,” on page 1003 to learn about OpenPages Loss Event Entry and [“Planning the configuration” on page 1003](#) to learn about decisions to make before you begin.

Procedure

1. Open the Loss Event Entry Configuration tool with the following URL.

```
http://<server>:<port>/openpages/app/jspview/lossevent#/editconfig
```

Log in with your OpenPages user account. You must be a member of the OPAdministrators user group to access the tool. You can have it open and simultaneously be logged in to OpenPages to work on other administration tasks. Click **Save** in the tool to refresh it with the most recent changes you make in OpenPages. For example, if you change information text in OpenPages and return to the Loss Event Entry Configuration tool, you do not see the changes until you click **Save**.

When you provide fields in the format, <Field Group>:<Field Name>, ensure that no spaces exist before and after the colon.

2. Complete the fields in the tool. Hover over a field to see a description.
3. Complete the fields in the **Object Types** section.
 - a) In **Loss Event View Name**, enter the name of a loss event creation view that is used to determine the information on the **Loss Event** tab. The default is LE Entry - LE.
 - b) In **Loss Impacts View Name**, enter the name of a loss impact creation view that is used to determine the information on the **Loss Impacts** tab. The default is LE Entry - LI. Click **Required** to make it mandatory for a user to enter information on the tab.

- c) In **Loss Recoveries View Name**, enter the name of a loss recovery creation view that is used to determine the information on the **Loss Recoveries** tab. The default is LE Entry - LR. Click **Required** to make it mandatory for a user to enter information on the tab.
 - d) For **Files**, click **Present** to show the **Files** tab. Users can click the **Files** tab to add attachments to a loss event. Clear **Present** to hide the **Files** tab. Click **Required** to make it mandatory for a user to attach at least one file.
4. Complete the fields in the **Locales** section for each locale.
- a) Click **Enabled** to allow users to access that locale.
 - b) Enter a **Password** for the dedicated, locale user.
- You must enter a password and save the configuration for users to be able to access OpenPages Loss Event Entry. The user password is automatically updated in OpenPages. To change the dedicated users' passwords in the future, use the Loss Event Entry Configuration tool rather than OpenPages.
- Important:** Do not change the dedicated users' passwords by using OpenPages. Always use the Loss Event Entry Configuration tool to change the passwords. If you change the passwords in OpenPages, users will not be able to use Loss Event Entry because the passwords will be out of sync.
- You can use the user names included in the out-of-the box system. If you change the user names in the Loss Event Entry Configuration tool, they must match the user names of the dedicated users.
- For each dedicated user, ensure that the **User cannot change password** and **Password never expires** options are enabled in OpenPages. To view these settings, go to **Administration > Users**, select a dedicated user, and then click **Reset password**.
5. Complete the fields in the **Other** section.
- a) In **Default Parent Path**, enter a path, for example, /Global Services/North America Banking, to the business entity that is the default parent of new loss events if users cannot or do not select a parent. Mandatory.
 - b) In **Parent Field Name**, enter the name of a Business Entity Selector field that users can use to select a parent business entity for a new loss event. Format is <Field Group>:<Field Name>. It must be included in the selected creation view, and it must have a display type of Business Entity Selector. The default is OPSS-LE-BE:Primary Caused Entity. If not given or the user does not select a value in this field, the value in **Default Parent Path** is used as the parent for a loss event.
 - c) In **Submitter Email Field Name**, enter the name of a field that email confirmations are sent to. It must be defined in the creation view and be a Text Box display type. The default is OPSS-LE-Contact:Your Email.
 - d) In **Default Triage Team**, enter the default users and user groups that loss events are assigned to for follow up. Can contain multiple actors separated by commas. Mandatory.
 - e) In **Triage Team Field Name**, enter the name of an actor field. Format is <Field Group>:<Field Name>. It must be defined in the creation view. Optional. If not given or the user does not select a value in this field, the value in **Default Triage Team** is used to assign a triage team to a loss event.
 - f) In **Populate Triage Team Field Name**, enter the field in which the triage team is stored. Format is <Field Group>:<Field Name>. The default is OPSS-LossEv:Owner. Mandatory. The selected actor or actors from either **Default Triage Team** or **Triage Team Field Name** are copied to the field given in the **Populate Triage Team Field Name**.
 - g) Select **Display Resource ID of Created Objects** to show a loss event's internal system-generated identifier to the user on the confirmation window and confirmation email.
 - h) Review the **Date Validation** rules that are delivered with the system and make changes, if needed.
- Follow these guidelines:
- You write the rules in the syntax <object type name>:<field group name>:<field name>. In all three portions use the item's name, not its label.
 - You can use the Loss Event or any of the other object types used by OpenPages Loss Event Entry. A rule cannot cross object types.
 - You can use: <= and >=.

- You can use the word TODAY.
 - You can use only date fields, and they must exist in the creation view.
- i) Select a **Default Locale**. This is the default locale if one is not specified in the URL. The default locale is listed first in the selection list, then all other locales are listed in alphabetical order in the user's language.
- j) In **Submitter Email Subject Parameters**, enter fields that are included in the subject of the confirmation notification email that is sent to the submitter. Default is System Fields:Name.
- You can choose any of the fields in the Loss Event profile. The Application Text that is located in lossevent.confirm.subject references these parameters.
- For information, see [“How confirmation emails are configured” on page 1009](#).
- k) In **Submitter Email Body Parameters**, enter fields that are included in the body of the confirmation email that is sent to the submitter. Default is OPSS-LE-Contact:Your Name, System Fields:Name, System Fields:Resource ID, System Fields:Description.
- You can choose any of the fields in the Loss Event profile. The Application Text that is located in lossevent.confirm.content references these parameters.
- For information, see [“How confirmation emails are configured” on page 1009](#).
6. Click **Validate** to verify the configuration. You cannot save the configuration if fatal errors exist. Resolve them and validate again. You can save the configuration if non-fatal errors exist.
- If you have numerous errors, the **OK** icon rolls to the bottom of the list and is not visible. In the browser settings, zoom out to make the screen small enough to access the OK icon.
7. Click **Save**. The **Last Saved** time stamp on the page is updated.

Chapter 35. Configuring IBM Watson Integrations

OpenPages can be integrated with IBM Watson Assistant, IBM Watson Language Translator, and a natural language processing service.

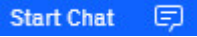
This video provides an overview of AI in OpenPages.

https://mediacenter.ibm.com/media/t/1_aawxeji2

IBM Watson Assistant

Configure an assistant and integrate it with OpenPages so that users can ask free-format questions and receive answers using a chat bot.

IBM Watson Assistant is a chat bot that can appear in the Task Focused UI. It can offer 24-hour support to the common questions that users have within OpenPages. It can provide interactive text answers, natural language search, and direct links to specific pages in OpenPages, for example, to a Creation View where a user can enter an Issue or Loss Event. A subscription to the IBM Watson Assistant service is required.

When an assistant is configured, the  icon is displayed on all pages in the Task Focused UI. It is displayed only to users with the application permission that allows them to access it.

Configuration overview

Complete the following steps to configure IBM Watson Assistant:

1. Configure an assistant. For more information, see [“Configuring a web chat assistant by using IBM Watson Assistant”](#) on page 1013.
2. Integrate the assistant with OpenPages. For more information, see [“Configuring the integration between an assistant and OpenPages”](#) on page 1014.

Show me how

This video provides an overview of using IBM Watson Assistant.

<https://youtu.be/NbvU-UdJ6Aw>

Configuring a web chat assistant by using IBM Watson Assistant

An assistant must be configured before it can be integrated with OpenPages.

Before you begin

Learn about IBM Watson Assistant using the extensive documentation, tutorials, and videos that IBM provides. For more information, see the [IBM Cloud documentation](#).

Choose a subscription for IBM Watson Assistant that includes the web chat interface. For example, the Assistant Plus subscription includes the web chat interface.

About this task

An assistant is a cognitive bot to which you add skills that enable it to interact with your users in useful ways.

The assistant must be saved with a web chat integration.

Note: You can create an assistant on IBM Cloud Pak for Data or on IBM Cloud.

Procedure

1. Create an assistant and configure skills that match the needs of OpenPages users.
2. Add a web chat integration to the assistant.

When you add a web chat integration, a code snippet is displayed in the **Add the chat UI to your web page** section. You need parts of the code snippet to integrate the assistant with OpenPages.

3. In **Customize your chat UI**, you can optionally change the style of the assistant. If you add an avatar image, make a note of the image URL because it must also be added in the OpenPages integration.

What to do next

Integrate the assistant with OpenPages. For more information, see [“Configuring the integration between an assistant and OpenPages”](#) on page 1014.

Configuring IBM Watson Assistant is an iterative process. As users work with it, you can improve and expand the skills. You might need to change or expand the skills as they change over time. You can also download a skills data usage report and improve it.

Configuring the integration between an assistant and OpenPages

Add integration information for an assistant so that it displays in the Task Focused UI in OpenPages.

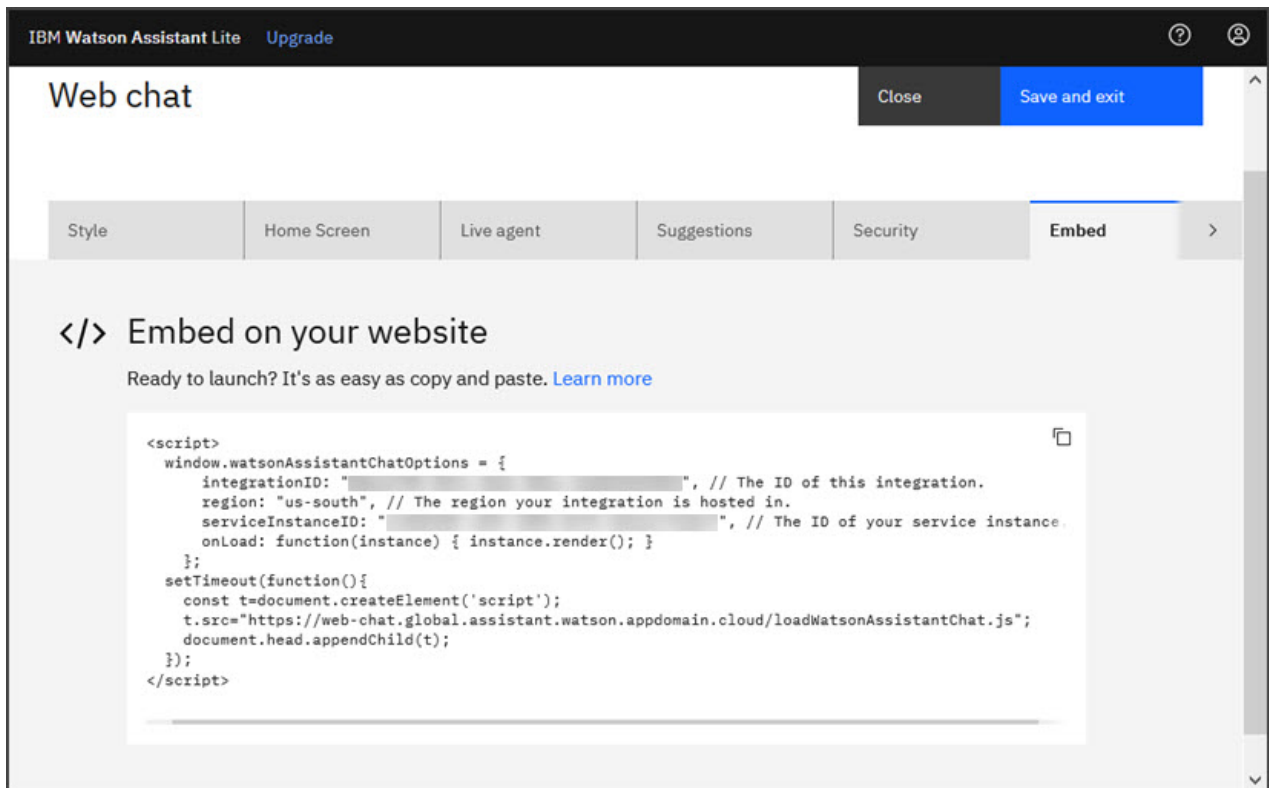
Before you begin

Add the **SOX > Administration > User Interfaces > Watson Assistant UI** application permission to role templates that are allowed to access IBM Watson Assistant .

Configure an assistant. For more information, see [“Configuring a web chat assistant by using IBM Watson Assistant”](#) on page 1013.

About this task

When an assistant is configured and saved with a web chat integration, a code snippet is displayed in the **Embed** section. You can import the code into the **Watson Assistant** page in OpenPages.



Procedure

1. Open the code snippet that is displayed when an assistant is saved with a web chat integration.
2. Click  > **Integrations** > **Watson Assistant**.
Or, in 8.2.0.3 and earlier, click  > **Watson Integrations** > **Watson Assistant**
3. Click .
4. Paste the code snippet into the **Configuration string** box, and then click **Import**.
The **Web Chat Options** table displays the values for your web chat assistant.
5. If the assistant is defined with an avatar image, enter the URL in **Assistant Image URLs**.
6. In **Assistant Profiles**, select the profiles that are allowed to access IBM Watson Assistant.
7. Click **Save**.
8. If you are using IBM Cloud Pak for Data, add your web chat URL to the list of allowed URLs in OpenPages.
 - a) In the **Web Chat Options** table, click **cloudPrivateHostURL** and copy its value.
 - b) Click  > **System Configuration** > **Settings**.
 - c) Click the **Applications** > **Assistant** > **Embedded Assistant URLs**
 - d) In the **Value** field, add the URL that you copied in step "8.a" on page 1015 to the list of URLs.
 - e) Click **Done**.

What to do next

Refresh the screen and test the assistant within OpenPages. Refine it as needed.

Tip: If the configuration of your assistant changes, you can re-import its code snippet. Or, you can edit the values in the **Web Chat Options** table.

Enabling additional security features for IBM Watson Assistant on IBM Cloud

IBM Watson Assistant has features around making sure that chat conversations are coming to IBM Watson Assistant from your web chat in an authorized way. You can turn on these additional security features for your web chat assistant. This task is optional.

About this task

For more information, see [Security](#) in the IBM Watson Assistant documentation.

Procedure

1. Generate RS256 2048-bit public and private keys.

For example, you can use OpenSSL to create the keys:

```
openssl genrsa -out private.pem 2048
openssl rsa -in private.pem -pubout -out public.pem
```

Save the keys. You need them in a later step.

2. Go to the configuration page for your web chat assistant on IBM Cloud or IBM Cloud Pak for Data.
3. Click the **Security** tab, and enable web chat security.

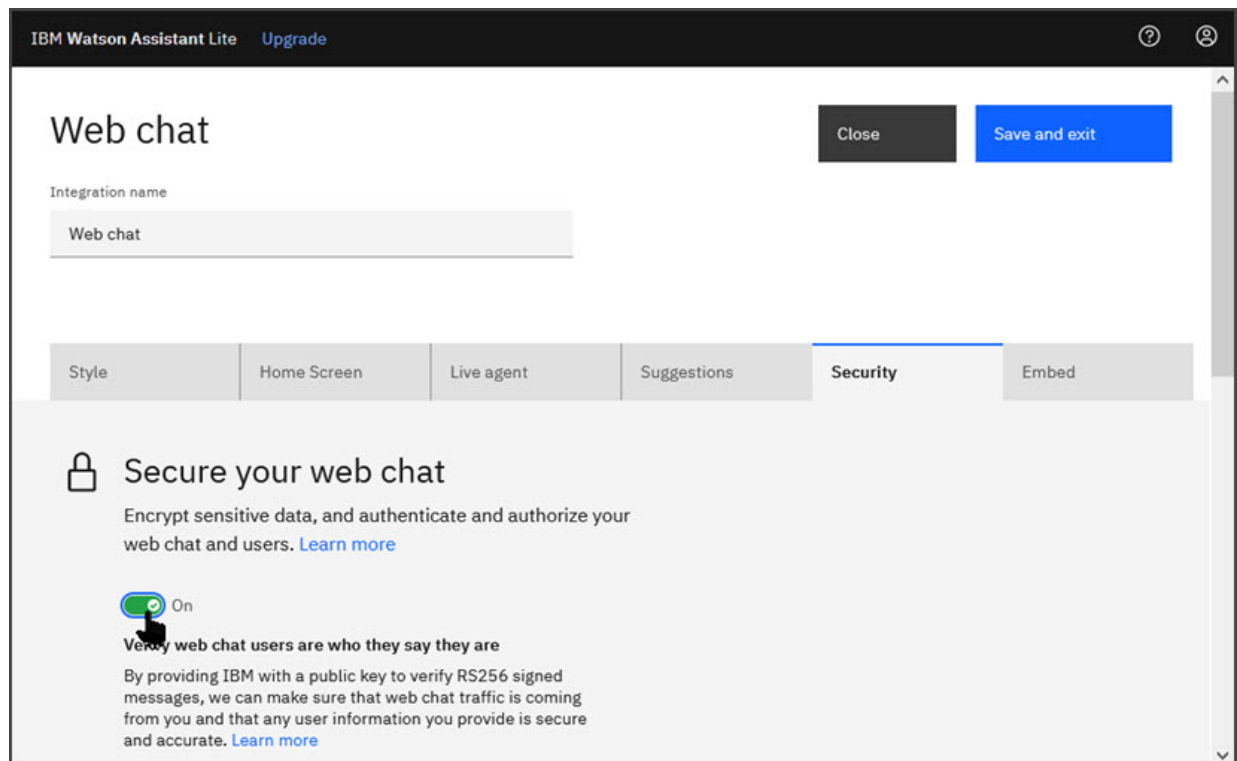


Figure 81. Enabling web chat security in IBM Watson Assistant

4. In the **Your public key** field, paste the public key that you created in step 1.

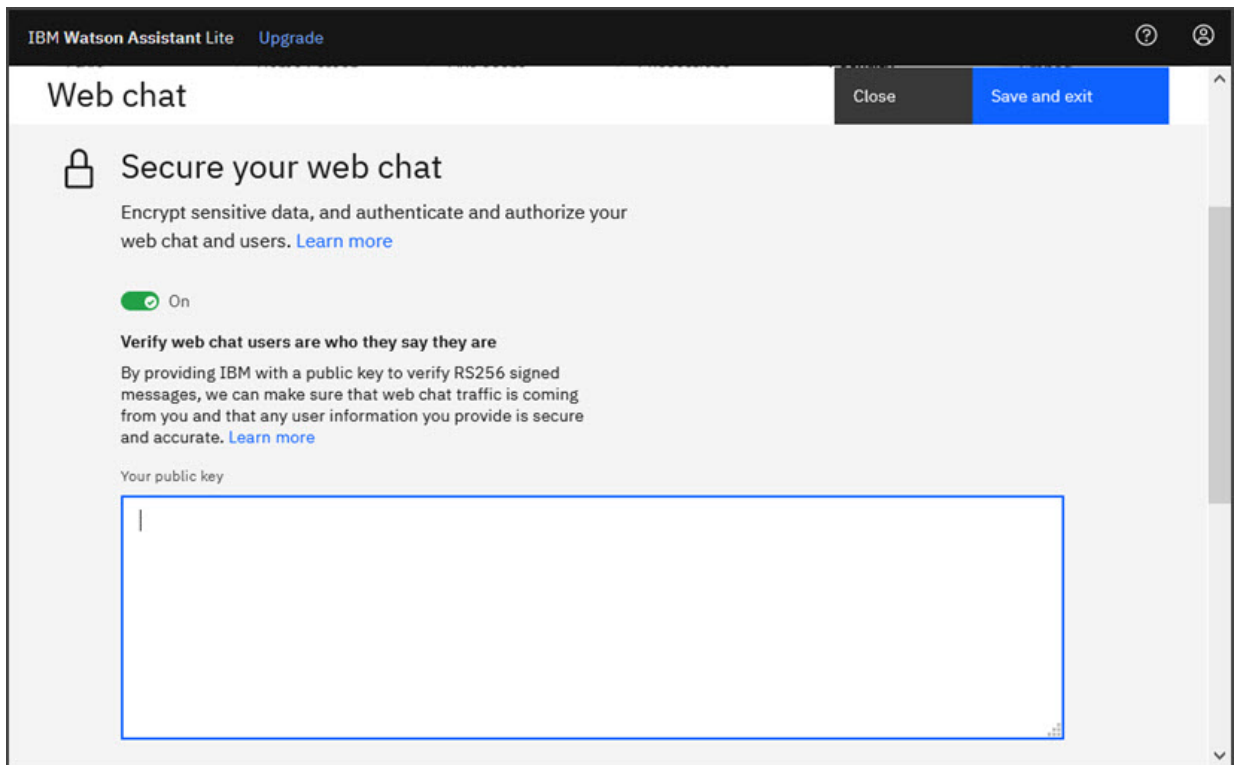


Figure 82. Adding your public key to your web chat assistant

5. Log in to OpenPages as a user with the **Watson Assistant** application permission.
6. Click  > **Integrations** > **Watson Assistant**.
7. In the **Private Key** field, paste the private key that you created in step 1.

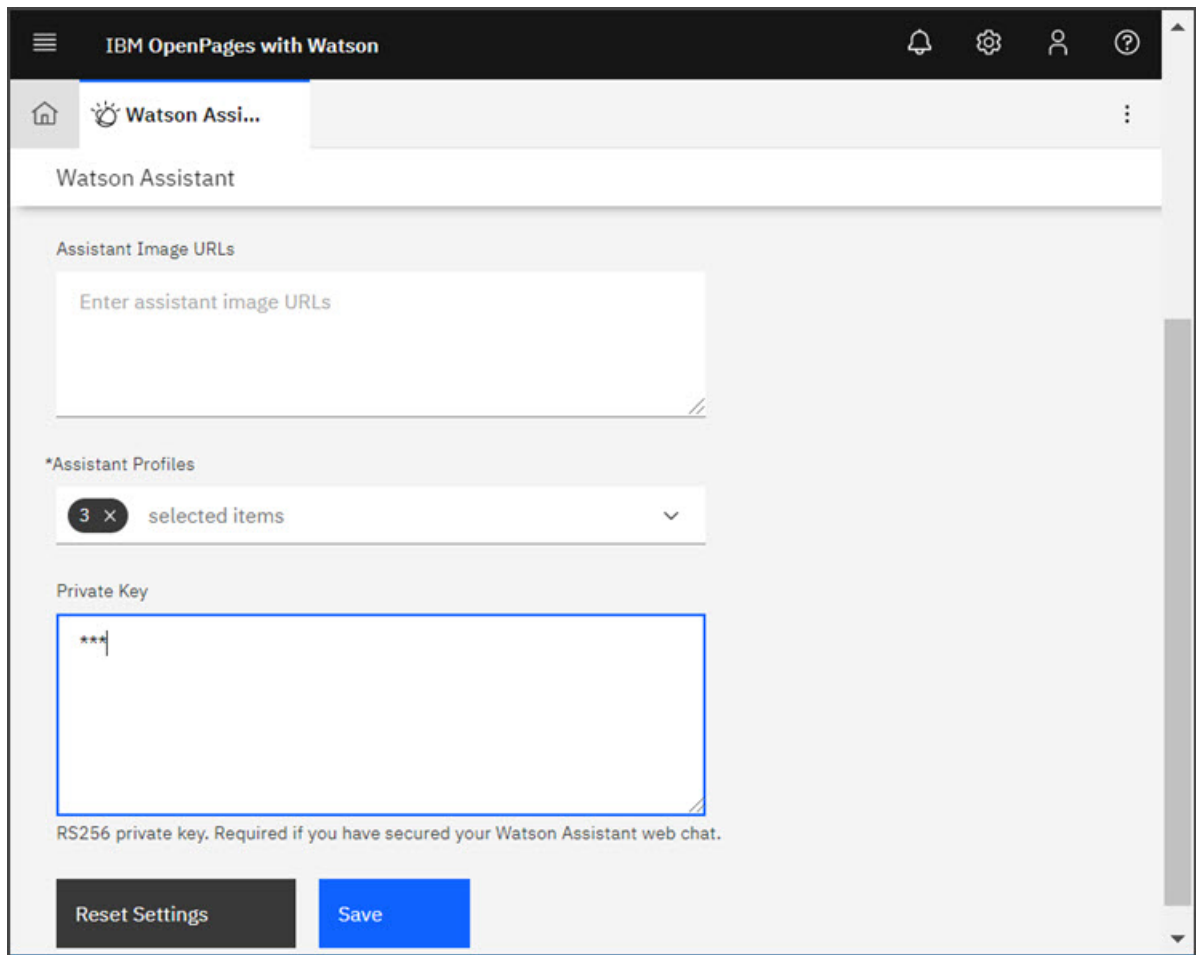


Figure 83. Adding your private key in OpenPages

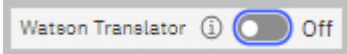
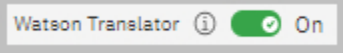
8. Click **Save**.

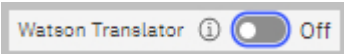
IBM Watson Language Translator

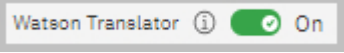
Configure IBM Watson Language Translator so that users and administrators can translate text as they work.

The icons and functionality for the IBM Watson Language Translator are different depending on whether the access point is for users or administrators.

How users interact with IBM Watson Language Translator

Users can work with translated text by using the  and  icons in Task Views.

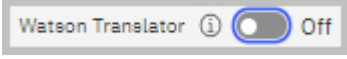
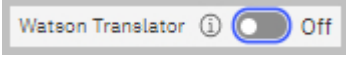
In a Task View, a user can click . Values in text fields are translated to the language associated to their locale. For each field that is translated, the user can toggle between the languages by clicking **View Original** and **View Translation**. Click the Info icon to view a confidence score.

Click  to turn off translated values.

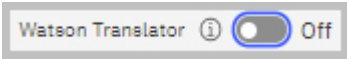
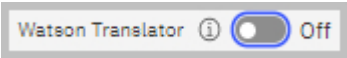
- Text field values (simple strings and long strings) are translated. Rich text fields and enumerated field values are not translated.
- There is no differentiation between US and UK English.

- Translated values on a Task View cannot be edited.
- They are not saved to the object.

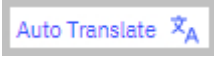
Example 1: a user's locale is set to U.S. English. The user views regulatory change objects in a Task View.

- First, the user views a regulatory change object that came from a French regulatory body. It contains field values in French. The user clicks the  icon. Text field values in French are translated to English.
- Next, the user views a regulatory change object that came from an EU regulatory body. It contains text field values in English, French, and Portuguese. The user clicks the  icon. The text field values in English remain unchanged. The text field values in French and Portuguese are translated into English.

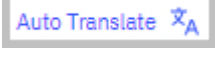
Example 2: a user's locale is set to Japanese. The user views regulatory change objects in a Task View.

- First, the user views a regulatory change object that came from a U.S. regulatory body. It contains field values in English. The user clicks the  icon. Text field values in English are translated into Japanese.
- Next, the user views a regulatory change object that came from an EU regulatory body. It contains field values in English, French, and Portuguese. The user clicks the  icon. Text field values are translated into Japanese.

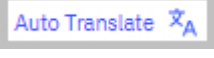
How administrators interact with IBM Watson Language Translator

Administrators can work with translated text by using the  icon on the following screens:

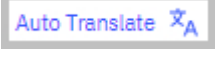
- Application Text
- Object Text
- Fields
- Dashboard configuration (administrators)
- View Designer
- GRC Workflow Designer

The  icon is available on screens where labels in multiple languages are defined. The original field value is translated into other languages. Translated values can be edited and they are saved.

Example 1: an administrator's locale is set to U.S. English. The administrator creates a new workflow using the GRC Workflow Designer.

- When defining stages in the workflow, the administrator enters a label in English and clicks **Edit**. Initially, the English text is displayed as label values for the other languages. The administrator clicks  and translated values are populated to the other languages. The administrator clicks **Done** to save the stage.

Example 2: an administrator's locale is set to Simplified Chinese. The administrator creates views using the View Designer.

- When defining elements in the view, the administrator enters a text value in Simplified Chinese and clicks **Edit**. Initially, the Simplified Chinese text is displayed as label values for the other languages. The administrator clicks  and translated values are populated to the other languages. The administrator clicks **Done** to save the values.

Configuration overview

Complete the following steps to configure IBM Watson Language Translator:

1. Configure IBM Watson Language Translator on IBM Cloud. For more information, see [“Configuring IBM Watson Language Translator on IBM Cloud”](#) on page 1020.
2. Configure the integration between IBM Watson Language Translator and OpenPages. For more information, see [“Configuring the integration between IBM Watson Language Translator and OpenPages”](#) on page 1020.

Configuring IBM Watson Language Translator on IBM Cloud

An IBM Watson Language Translator service must be configured before it can be integrated with OpenPages.

Before you begin

Learn about IBM Watson Language Translator using the extensive documentation, tutorials, and videos that IBM provides. For more information, see the [IBM Cloud documentation](#).

You can choose any pricing plan. If you have specific translation requirements, for example, complex legal texts, you may want to choose a plan that you can train.

Procedure

1. Create an IBM Cloud account if one does not already exist.
2. Log in, create the service, and get your service URL and API key. You need them later when you configure IBM Watson Language Translator in OpenPages.

After you create an instance of the IBM Watson Language Translator service, you can view the service URL and API key by going to the service dashboard, finding the service, and clicking **Manage** and **Show Credentials**.

3. Depending on the pricing plan you chose, you might be able to train the IBM Watson Language Translator service.

What to do next

Complete the remaining tasks that are described in [“IBM Watson Language Translator”](#) on page 1018.

Configuring the integration between IBM Watson Language Translator and OpenPages

Define integration information for IBM Watson Language Translator so that it can be used in the Task Focused UI in OpenPages.

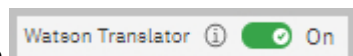
Before you begin

You need a IBM Watson Language Translator service. For more information, see [“Configuring IBM Watson Language Translator on IBM Cloud”](#) on page 1020.

Set the following application permissions:

- Set the **Watson Language Translator** permissions for administrators who are allowed to access the  > **Integrations** > **Watson Language Translator** menu item.
- Set the **Watson Language Translator UI** permission for users who are allowed to use IBM Watson

Language Translator to view translated text in Task Views by using the



icon. It also allows access to the  icon from administrator tasks.

For more information, see [“Types of application permissions”](#) on page 91.

Procedure

1. Get the service URL and API key for the IBM Watson Language Translator service. For more information, see [“Configuring IBM Watson Language Translator on IBM Cloud”](#) on page 1020.
2. Click  > **Integrations** > **Watson Language Translator**.
Or, in 8.2.0.3 and earlier, click  > **Watson Integrations** > **Watson Language Translator**
3. Copy the IBM Watson Language Translator service URL into **Service URL**.
4. Optional: Type the IBM Watson Language Translator API version into **API Version**.
To use the default value that is used by OpenPages, leave the field empty.
For more information, see [Versioning](#) in the IBM Watson Language Translator documentation.
5. Copy the IBM Watson Language Translator API key into **API Key**.
6. In **Confidence Threshold** enter the lowest confidence score that a suggestion must meet. This is a confidence score for recognizing a particular language. It is not a confidence score of the quality of the translated text.
7. Define the object types that are allowed to be translated.
 - To enable translation for all object types, set **Enable all Object Types** to true.
 - To restrict translation to specific object types, set **Enable all Object Types** to false. Under **Object Types**, click the check box next to each object type that is allowed to be translated.
8. Click **Save**.
9. Click **Test Connection** to check the connection.
10. Test the functionality across the system.

Results

Note: Should you ever want to turn off the IBM Watson Language Translator feature after it has been configured, clear the **Watson Language Translator UI** permission on users. The buttons for the IBM Watson Language Translator are then hidden.

Natural language processing services

Configure a natural language processing service and integrate it with OpenPages so that users have support when they classify objects and make object associations. A natural language processing service understands the intent behind text and returns suggestions, together with a confidence score.

The following natural language processing services are supported:

- IBM Watson Discovery in IBM Cloud Pak for Data
- IBM Watson Natural Language Understanding in IBM Cloud (8.2.0.4 and later)
- Natural Language Classifier service in IBM Cloud

Note: If you are setting up a new natural language processing service, use IBM Watson Natural Language Understanding instead of the Natural Language Classifier service.

You can configure a natural language processing service to suggest either taxonomy classifications or parent and child object associations. You can use it for any objects in OpenPages but it is typically used to classify loss events, waivers, issues, and incidents or to associate them to a risk, policy, or control.

If you configure it to suggest taxonomy classifications, you can use it, for example, to support users when they classify a loss event to the correct Basel II categorization or when they classify waivers as exceptions to regulatory compliance. The text description that a user enters is used as input to a natural language processing service that has been trained with knowledge from your domain specialists.

If you configure it to suggest object associations, you can use it to support users when they, for example, create an Issue object and need to associate it to a parent Control object. Again, the text description that a user enters is used as input to a natural language processing service but in this case it returns a suggested parent Control object together with a confidence score. Object association suggestions can be configured to suggest either parent or child associations. They are synchronized with associations that users make for parent or child objects.

Using a natural language processing service is best suited to situations where users are generating a high volume of objects, hundreds or even thousands per year. Cognitive computing adds value when it is scaled to a large data set and to a large group of users. The data the classifier is trained on should be relatively small and static. For example, you would want to train a classifier to provide object association suggestions to a small number of Controls in the Controls Library, which is small and relatively static, rather than to all the Controls in your business, which are numerous and dynamic. You would not want to train a classifier to make object associations between objects that change rapidly, for example, Audit Findings and Issues, because Issues are constantly changing and there might be thousands of them.

You can link OpenPages to one or more services, either to support different purposes or multiple languages.

A natural language processing service and classifier fields are accessed from both the Task Focused UI and the Standard UI. The results are the same but how they are displayed is slightly different. IBM Watson Discovery is not sported in the Standard UI.

Terms to understand

natural language processing service

A natural language processing service uses machine learning algorithms to return the top-matching predefined classes for short text inputs.

IBM Watson Discovery

IBM Watson Discovery is a natural language processing service on IBM Cloud Pak for Data. You configure a IBM Watson Discovery service and then integrate it with OpenPages. It uses the Analyze API.

IBM Watson Natural Language Understanding

IBM Watson Natural Language Understanding is a language processing service in IBM Cloud. You can train and deploy text classifier models and then integrate them with OpenPages. IBM Watson Natural Language Understanding learns from your data and can predict classifications for texts that it is not trained on. IBM Watson Natural Language Understanding is similar to the Natural Language Classifier, but unlike the Natural Language Classifier, IBM Watson Natural Language Understanding is a multi-label, multi-class classifier. It assumes that text likely belongs to more than one class and can better predict texts with multiple classifications.

Natural Language Classifier

A Natural Language Classifier service is a Watson natural language processing service in IBM Cloud. You configure and train a Natural Language Classifier service and then integrate it with OpenPages. A Natural Language Classifier service learns from your data and then can return information for texts that it is not trained on.

Classifier Configuration

A classifier configuration in OpenPages defines connection information to an instance of a natural language processing service. For taxonomy classifications, it specifies the classifier target fields for the instance. For object associations, it specifies the object type to associate, whether it is a child or parent relationship, and other attributes.

Classifier Field

A classifier field is a field group in OpenPages that contains the name of a classifier configuration and a classifier input field. In the Task Focused UI, an IBM Watson Insights button is displayed in place of a classifier field (taxonomy classifications) or as an action (object associations). In the Standard UI, the **View Suggestions** button is displayed next to a classifier field.

Classifier Input Field

A classifier input field is a field in OpenPages that contains the short text input that a natural language processing service interprets and classifies. It is typically a **Description** field. The text *Adding a description improves IBM Watson Suggestions* is automatically displayed below a classifier input field.

Classifier Target Fields

For taxonomy classifications, classifier target fields are fields in OpenPages that are set when a user chooses suggestions for a classifier field.

Watson Insights

In the Task Focused UI, the underlying infrastructure in OpenPages is tied to IBM Watson Insights. An IBM Watson Insights button is displayed and suggestions are displayed in a **Watson Insights** panel.

An IBM Watson Insights button appears only if the Natural Language Classifier is able to make a suggestion based on the text entered. The button does not appear if the text does not generate suggestions.

The user interaction in the **Watson Insights** panel is the same regardless of whether the service is IBM Watson Discovery or a Natural Language Classifier.

Configuration overview for natural language classifier services

To use OpenPages together with a natural language processing service, you must design how you want the system to work and complete several configuration tasks.

Before you begin

- Decide what type of service to use:
 - IBM Watson Discovery in IBM Cloud Pak for Data
 - IBM Watson Natural Language Understanding in IBM Cloud (8.2.0.4 and later)
 - Natural Language Classifier service in IBM Cloud
- **Note:** If you are setting up a new natural language processing service, use IBM Watson Natural Language Understanding instead of the Natural Language Classifier service.
- Decide the purpose of the classifier: taxonomy suggestions or object association suggestions.
- Verify that the application server has outgoing internet access so that it can communicate with a Natural Language Classifier service.
- Verify that the data type for the classifier input field is Simple String.
- If the classifier is for taxonomy suggestions:
 - Decide what area you want to support, for example, helping users select Basel II categorizations.
 - Decide what objects the classifier field is available on, for example, loss events, waivers, issues, and incidents.
 - Verify that the data type for the classifier target fields is Enumerated String. You can have up to three classifier target fields.
 - Decide whether you want to allow users to select one or many suggestions. Set **Multi-valued** to false on at least one of the classifier target fields to allow users to select only one suggestion. Set **Multi-valued** to true on all classifier target fields to allow multiple selections.
- If the classifier is for object association suggestions:
 - Decide on the object types and associations that you want to use. For example, suppose you want to create a classifier that helps users to map issues to controls. In this case, you need the classifier to analyze the description of the issue objects, and then suggest parent controls for the issues.
 - Decide what objects the classifier field is available on. For example, if you're mapping issues to controls, the classifier field needs to be available on issues.
 - Verify the path to the object type that you want to associate to. For example, if you're mapping issues to controls, verify the path of the controls.

- Decide what names and descriptions are displayed when a user selects an object.

About this task

The following steps describe how to configure a natural language processing service.

Procedure

1. Configure and train the natural language processing service.
 - IBM Watson Discovery . For more information, see [“Configuring Watson Discovery ”](#) on page 1025.
 - IBM Watson Natural Language Understanding in IBM Cloud (8.2.0.4 and later)
 - Natural Language Classifier service on IBM Cloud. For more information, see [“Configuring a Natural Language Classifier on IBM Cloud”](#) on page 1026.
2. Define a classifier configuration. This step can be done in either user interface. For more information, see [“Defining a Classifier Configuration \(Task Focused UI\)”](#) on page 1028 and [“Defining a Classifier Configuration \(Standard UI\)”](#) on page 1029.
3. Define a classifier field. For more information, see [“Defining a classifier field”](#) on page 1030.
4. If it is not already there, add the classifier field's field group to the object type.
5. Add the classifier field to the profile.
6. In the Task Focused UI, add the classifier field to views where you want it to display. For more information, see [“Adding a classifier field that makes taxonomy suggestions ”](#) on page 410 and [“Adding a classifier field that makes object association suggestions”](#) on page 430.
7. In the Standard UI, add the classifier field to views where you want it to display. You can add it to Detail, Activity, and Add New views. You can also add it to Loss Event Entry. On these views, ensure that **Read-Only** is cleared so that the fields are editable. On the Add New view, although you can place the classifier field anywhere, you might want to place it immediately following the description field where users enter the text input. You can also add it to Filtered List Views, Grid, Context, List views, and to home page portlets. On these views classifier fields are read-only.
8. Optional: If the classifier is for taxonomy suggestions, add the classifier target fields to views in the Standard UI where you want them to display. Ensure that **Read-Only** is cleared so that the fields are editable. On the Detail and Add New views, although you can place the classifier target field anywhere, you might want to place them immediately following the classifier field. You can also choose not to display the classifier target fields on the views.
9. Re-create the reporting framework so you can access usage data in Cognos. Do this only one time, not for every service you configure. For more information, see [“Generating the reporting framework ”](#) on page 974.
10. Test the configuration and resolve errors.

If you encounter connection issues, import the Watson certificate into the WebSphere Liberty truststore. Do this only one time, not for every service you configure. For more information, see [“Importing a Watson certificate to the local truststore ”](#) on page 1031.

What to do next

After the service is in use, you can download data and monitor performance. For more information, see [“Monitoring and downloading classifier data usage ”](#) on page 1031.

A natural language processing service is in one language. IBM supports a fixed set of languages. You can use multiple services simultaneously, either for different purposes or to support multiple languages for the same purpose.

If you use multiple services for taxonomy suggestions, each service requires a unique classifier configuration, classifier field, and classifier output fields. A classifier input field can be used in more than one classifier field. However, ensure that each classifier configuration updates different classifier target fields. Do not define multiple classifier configurations that update the same classifier target fields.

For object associations, you must configure a service for each object type and relationship that you want to support. For example, if you want to provide parent association suggestions to Control objects and child association suggestions to Risk objects, you need two services. You can have multiple services per object type. Each service requires a unique classifier configuration and classifier field. A classifier input field can be used in more than one classifier field.

Configuring Watson Discovery

To use a IBM Watson Discovery service with OpenPages, you must configure it on IBM Cloud Pak for Data.

About this task

Learn about cognitive technology, IBM Watson Discovery , and the Analyzer API. IBM provides extensive documentation, tutorials, and videos for IBM Watson Discovery . For more information, see the [IBM Watson Discovery documentation](#).

IBM Watson Discovery must be version 3.5 or greater.

An IBM Watson Discovery service cannot be used with the Standard UI.

For information about the format to use when you are building the training data, see [Data Format - OpenPages Classifier Models](#).

For information about training and integrating classifier models using a IBM Watson Discovery service with OpenPages, see [Training and integrating AI classifier models on OpenPages - Watson Discovery Analyze API](#).

Configuring a Natural Language Understanding service on IBM Cloud

To use a Natural Language Understanding service with OpenPages, you must configure it on IBM Cloud (formerly called Bluemix).

Before you begin

Learn about cognitive technology and IBM Cloud. IBM provides extensive documentation, tutorials, and videos for the Natural Language Understanding. For more information, see [Getting started with Natural Language Understanding](#).

About this task

A Natural Language Understanding service is empty when you begin and must be trained for what you want to classify. If, for example, you want to help users correctly classify loss events to the correct Basel II categorization, you map short texts that they might write to the correct Basel II categories. The challenge when you create training data is to write short text inputs that reflect how users describe various loss events. The Natural Language Understanding service does not simply search through the texts, but instead interprets their meaning. When the meaning of a text is matched to a classification, it has a higher confidence score.

Procedure

1. Create a IBM Cloud account if one does not already exist.
2. Log in, create the service, and get your service URL and API key. You need the service URL and API key later when you define a classifier configuration in OpenPages. Also make a note of the classifier instance ID.

After you create an instance of the Natural Language Understanding service, you can view the service URL and API key by clicking **Manage** and **Show Credentials** from the left pane of the service dashboard.

3. Build the training data. For information about the format of the data, see [Data Format - OpenPages Classifier Models](#).

4. Train the model. For information about training, see [Training and integrating AI classifier models on OpenPages - Natural Language Understanding \(NLU\)](#).

What to do next

Complete the remaining tasks that are described in [“Configuration overview for natural language classifier services”](#) on page 1023.

Configuring a Natural Language Classifier on IBM Cloud

To use a Natural Language Classifier with OpenPages, you must configure it on IBM Cloud (formerly called Bluemix).

Before you begin

Learn about cognitive technology and IBM Cloud. IBM provides extensive documentation, tutorials, and videos for the Natural Language Classifier. For more information, see the [IBM Cloud documentation](#).

About this task

A Natural Language Classifier service is empty when you begin and must be trained for what you want to classify. If, for example, you want to help users correctly classify loss events to the correct Basel II categorization, you map short texts that they might write to the correct Basel II categories. The challenge when you create training data is to write short text inputs that reflect how users describe various loss events. The Natural Language Classifier does not simply search through the texts, but instead interprets their meaning. When the meaning of a text is matched to a classification, it has a higher confidence score.

Procedure

1. Create a IBM Cloud account if one does not already exist.
2. Log in, create the service, and get your service URL and API key. You need the service URL and API key later when you define a classifier configuration in OpenPages. Also make a note of the classifier instance ID.

After you create an instance of the Natural Language Classifier service, you can view the service URL and API key by clicking **Manage** and **Show Credentials** from the left pane of the service dashboard.

3. Build the training data. Define the short text inputs and map them to classifications. The training data must be in a CSV file. The first column in the file is the short text input to classify. The additional columns are classes that apply to that text.

If the classifier is for taxonomy suggestions, define the short text inputs and map them to classifications. The training data must be in a CSV file. The first column in the file is the text to classify. The additional columns are classes that apply to that text. The number of classes must be equal to the number of classifier target fields that you define in the classifier configuration. If you set up three classifier target fields, as in the following example, you must have three classes.

Table 304. Example training data for taxonomy suggestions			
Short text input	Class 1	Class 2	Class 3
Checks were forged	Internal Fraud	Theft and Fraud	Forgery
Check kiting	Internal Fraud	Theft and Fraud	Check kiting
Smuggling	Internal Fraud	Theft and Fraud	Smuggling
External party stole assets	External Fraud	Theft and Fraud	Theft/Robbery

Table 304. Example training data for taxonomy suggestions (continued)			
Short text input	Class 1	Class 2	Class 3
Product defect	Clients, Products and Business Practices	Product Flaws	Product Defects
Model error	Clients, Products and Business Practices	Product Flaws	Model Errors

If the classifier is for object associations, define the short text inputs and map them to object types. The training data must be in a CSV file. The first column in the file is the short text. The second column is the system name of the object that applies to that text.

Table 305. Example training data for object association suggestions	
Short text input	Class
Key Management	10.1.2 Key management
Cryptographic key management	10.1.2 Key management
Key management system should be storing keys	10.1.2 Key management
Key management system should be backing up or archiving keys	10.1.2 Key management
Key management system should be destroying keys	10.1.2 Key management
Key management system should be backing up or archiving keys	10.1.2 Key management
Security perimeters should be defined	11.1.1 Physical security perimeter
Clear desk policy	11.2.9 Clear desk and clear screen policy
Clear screen policy	11.2.9 Clear desk and clear screen policy

4. Load the CSV file into the Natural Language Classifier service you created on IBM Cloud.
5. Train the classifier. After it is trained, IBM Cloud assigns it a classifier ID. You need the classifier ID later when you define a classifier configuration in OpenPages. Every time that you train the classifier, you get a new classifier ID.
6. Ensure that the service is running.

What to do next

Complete the remaining tasks that are described in [“Configuration overview for natural language classifier services”](#) on page 1023.

Training the classifier is an iterative process. As users work with it, you can improve and expand the short text inputs. You might need to change or expand the categorizations as they change over time. You can also download classifier usage and improve it. For more information, see [“Monitoring and downloading classifier data usage”](#) on page 1031.

Optionally, set up more security, for example, use a firewall to restrict access to IBM Cloud. For information, see [How do I know that my data is safe?](#) .

Defining a Classifier Configuration (Task Focused UI)

A classifier configuration defines connection information for an instance of IBM Watson Discovery or the Natural Language Classifier on IBM Cloud.

Before you begin

Configure the service that you want to connect to. For more information, see [“Configuring Watson Discovery” on page 1025](#) and [“Configuring a Natural Language Classifier on IBM Cloud” on page 1026](#). Make a note of the API key and the ID of the natural language classifier instance that you created.

Procedure

1. Click  > **Integrations** > **Mapping and Taxonomy Suggestions**.
Or, in 8.2.0.3 and earlier, click  > **Watson Integrations** > **Mapping and Taxonomy Suggestions**.
2. Click **New Classifier**.
3. Complete the fields in the **Classifier Information** section.
 - a) Select Watson Discovery Analyze API or Natural Language Classifier in **Watson Service Type**.
 - b) In **Type**, select Enumeration (taxonomy suggestions) or Association (object association suggestions).
 - c) In **Name**, enter a name.
 - d) In **Description**, enter descriptive information.
 - e) Enter a link in **Link**. The link is optional and for information purposes only. The default is `http://www.cloud.ibm.com`.
4. For a IBM Watson Discovery service, complete the fields in the **IBM Watson Discovery Service** section.
 - a) Type your service URL in **URL for Request**. It is the URL to the IBM Watson Discovery Service on IBM Cloud Pak for Data that you configured.
 - b) Type the **Project ID**.
 - c) Type the **Collection ID**.
 - d) Enter a **Username**.
 - e) Enter a **Password**.
 - f) Enter an **API Version**.
5. For a Natural Language Understanding service, complete the fields in the **IBM Watson Natural Language Understanding Service** section. The person who trained the classifier model will have this information.
 - a) Type your service URL in **URL for Request**. It is the URL to the Natural Language Understanding service on IBM Cloud.
 - b) In **API Key**, enter the API key of the Natural Language Understanding instance.
 - c) In **Model ID**, enter the identifier of the Natural Language Understanding classifier model.
6. For a Natural Language Classifier service, complete the fields in the **IBM Watson Natural Language Classifier Service** section.
 - a) Type your service URL in **URL for Request**. It is the URL to the Natural Language Classifier on IBM Cloud.
 - b) In **API Key**, enter the API key of the Natural Language Classifier instance that you created.
 - c) In **Model ID**, enter the identifier of the Natural Language Classifier instance that you created and trained.
7. In the **Usage Information** section, in **Confidence Threshold** enter the lowest confidence score that a suggestion must meet.

8. If **Type** is set to Enumeration, in the **Field Settings** section you can choose up to three fields. The order of the fields is important. Select the top-level field first, then the second-level field, and so on.
9. If **Type** is set to Association, complete the **Association** section:
 - a) In **Object Type**, select the object type that is associated, for example, SOXControl.
 - b) In **Association Type**, select Child or Parent.
 - c) In **Object Path**, enter a path to directories to search, for example, /Library.
 - d) In **Name Field**, specify the field that is displayed as the object's name after a user selects an object to associate, for example, System Fields.Name. Format is <Field Group>.<Field Name>.
 - e) In **Description Field**, specify the field that is displayed as the object's description after a user selects an object to associate, for example, System Fields.Description. Format is <Field Group>.<Field Name>.
10. Click **Create**.

What to do next

Complete the remaining tasks that are described in [“Configuration overview for natural language classifier services” on page 1023](#).

Defining a Classifier Configuration (Standard UI)

A classifier configuration defines connection information for an instance of the Natural Language Classifier on IBM Cloud.

Before you begin

Configure the Natural Language Classifier that you want to connect to. For more information, see [“Configuring a Natural Language Classifier on IBM Cloud” on page 1026](#). Make a note of the API key and the ID of the natural language classifier instance that you created.

Procedure

1. Click **Administration > Cognitive Services > Natural Language Classifiers**.
2. Click **New**.
3. Complete the fields in the **Classifier Information** section.
 - a) In **Name**, enter a name.
 - b) In **Description**, enter descriptive information.
 - c) In **Link**, enter a link to the training page in IBM Cloud where you can add training data. The link is optional and for information purposes only. The default is `http://www.cloud.ibm.com`.
 - d) In **Type**, select Enumeration (taxonomy suggestions) or Association (object association suggestions).
4. Complete the fields in the **IBM Watson Natural Language Classifier Service** section.
 - a) Type your service URL in **URL for Request**. It is the URL to the Natural Language Classifier on IBM Cloud.
 - b) In **API Key**, enter the API key of the Natural Language Classifier instance that you created.
 - c) In **ID**, enter the identifier of the Natural Language Classifier instance that you created and trained.
5. In the **Usage Information** section, in **Confidence Threshold** enter the lowest confidence score that a suggestion must meet.
6. If **Type** is set to Enumeration, in the **Field Settings** section you can provide up to three fields in **Classifier Target Field**. Format is <Field Group>.<Field Name>. The order of the fields is important. Place the top-level field first, then the second-level field, and so on.
7. If **Type** is set to Association, complete the **Association** section:

- a) In **Object Type**, enter the name of the object type that is associated, for example, SOXControl.
- b) In **Association Type**, select Child or Parent.
- c) In **Object Path**, enter a path to directories to search, for example, /Library.
- d) In **Name Field**, specify the field that is displayed as the object's name after a user selects an object to associate, for example, System Fields.Name. Format is <Field Group>.<Field Name>.
- e) In **Description Field**, specify the field that is displayed as the object's description after a user selects an object to associate, for example, System Fields.Description. Format is <Field Group>.<Field Name>.

Results

The system saves the classifier configuration as a JSON file. To make changes, use the **Administration > Cognitive Services > Natural Language Classifiers** task. Do not edit the JSON files directly.

What to do next

Complete the remaining tasks that are described in [“Configuration overview for natural language classifier services” on page 1023](#).

Defining a classifier field

A classifier field contains the name of a classifier configuration and a classifier input field.

Before you begin

Define a classifier configuration. For more information, see [“Defining a Classifier Configuration \(Task Focused UI\)” on page 1028](#).

About this task

A classifier field is a field whose **Data Type** is set to Classifier. Like other fields in OpenPages, you must add them to views and profiles. For more information, see [Chapter 9, “Fields and field groups,” on page 199](#).

You can use FastMap to import and export classifier fields and the values for suggestions in associated classifier target fields. This is typically done during a migration process. Do not change the classifier field or the values for suggestions after you export and before you reimport.

Procedure

1. Follow the instructions in [“Defining fields and adding them to field groups” on page 207](#).
2. Click **New** to create a new field.
 - a) In **Data Type**, select Classifier.
 - b) In **Classifier Configuration Name**, enter the name of the classifier configuration that you created in [“Defining a Classifier Configuration \(Task Focused UI\)” on page 1028](#).
 - c) In **Classifier Input Field**, enter the field that contains text to be interpreted by a service, for example, System Fields.Description. Format is <Field Group>.<Field Name>.
3. Save the field.

What to do next

Complete the remaining tasks that are described in [“Configuration overview for natural language classifier services” on page 1023](#).

Monitoring and downloading classifier data usage

After a natural language processing service has been implemented, you can monitor data usage and make improvements. You can view what users are searching for and what suggestions they select.

Procedure

1. Click **Reporting > Team content > OPENPAGES_REPORTS_V6 > General Reporting > General Reporting (Relational) > Audit Trail > Classifier Audit Trail**.
2. Click **Insert**.

The results show all requests that were sent to a classifier. Analyze the following columns:

- **Text sent to Classifier** are the descriptions users entered.
- **Selected Suggestion** are the suggestions that users chose.
- **Confidence** is the confidence score that the classifier returned for the selected suggestion.
- **Classifier Results** are the suggestions that the classifier issued for a description.

What to do next

Use the results to improve the classifier. You can download the usage data as a CSV file and use it as a basis for new training data for the natural language processing service.

Importing a Watson certificate to the local truststore

You might need to import a Watson certificate to the local truststore. Do this task if you encounter connection issues between the OpenPages with Watson servers and the Watson server on IBM Cloud.

Before you begin

- Obtain the URL of the secure target server, in this case the Watson server. You can verify it on [IBM Cloud](#). The target secure server is your service URL, for example `api.<location>.<offering>.watson.cloud.ibm.com`.
- The target secure server application from which you are going to retrieve the certificate must be running and listening on the port.

About this task

Complete this step even if you do not use TLS/SSL. The root certificate contains the public key and has been verified by the certificate authority (CA).

Procedure

1. Get the certificate from the Watson server.

You can use your browser to get the certificate or you can use OpenSSL.

For example:

```
openssl s_client -servername <service_url> -connect <service_url>:443 </dev/null 2>/dev/null  
| sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > watson-nlc.pem;
```

2. Use Keytool to import the certificate into your WebSphere Liberty truststore.

For example:

```
keytool -import -alias watson-nlc -trustcacerts -file watson-nlc.pem -keystore  
<keystore_path> -storetype PKCS12 -storepass <keystore_password> -noprompt
```

In OpenPages with Watson, the default path is `<OP_HOME>/wlp-user/servers/
<server_name>Server<#>/resources/security/`

3. Get the certificate from `https://iam.bluemix.net`.

You can use your browser to get the certificate or you can use OpenSSL.

For example:

```
openssl s_client -servername https://iam.bluemix.net -connect https://iam.bluemix.net:443
</dev/null 2>/dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > watson-
bluemix.pem;
```

4. Use Keytool to import the certificate into your WebSphere Liberty truststore.

For example:

```
keytool -import -alias watson-bluemix -trustcacerts -file watson-bluemix.pem -keystore
<keystore_path> -storetype PKCS12 -storepass <keystore_password> -noprompt
```

In OpenPages with Watson, the default path is `<OP_HOME>/wlp-user/servers/`
`<server_name>Server<#>/resources/security/`

5. Restart the OpenPages with Watson services.
6. If you are using a clustered environment, repeat these steps on each application server.

Chapter 36. IBM OpenPages Data Privacy Management

IBM OpenPages Data Privacy Management (DPM) solution is used by an organization to aid in complying with data privacy regulations. With DPM, you can maintain an inventory of all private data across the organization within OpenPages by using an integration with Watson Knowledge Catalog.

The integration imports metadata from Watson Knowledge Catalog into OpenPages. The data itself is not imported.

Note: To integrate with Watson Knowledge Catalog, you must meet the following prerequisites:

- You must have a Watson Knowledge Catalog instance on IBM Cloud Pak for Data.
- You must install IBM OpenPages Data Privacy Management. For more information, see [“Installing IBM OpenPages Data Privacy Management”](#) on page 1034.

Before you import data from Watson Knowledge Catalog, do the following tasks:

- In Watson Knowledge Catalog, create at least one catalog. Add assets to the catalog.
- In Watson Knowledge Catalog, classify the assets. Make a list of the classifications that you want to import into OpenPages.
- Optional: In OpenPages, create a questionnaire template to use for privacy assessments.

When you import data from Watson Knowledge Catalog, the data is mapped to the following object types in OpenPages:

Table 306. Watson Knowledge Catalog content mapping	
Watson Knowledge Catalog content...	Is loaded as a...
Project	Control Plan
Asset	Resource

When OpenPages imports data from Watson Knowledge Catalog, it does the following tasks:

- For projects, the import process does the following tasks:
 - Identifies projects that contain assets with one or more of the classifications that you configured for the import.
 - If the project does not exist in OpenPages, the import process creates a new Control Plan object.
- For assets, the import process does the following tasks:
 - Identifies assets with one or more of the classifications that you configured for the import.
 - If the asset does not exist in OpenPages, the import process creates a new Resource object and starts the Data Privacy Assessment workflow.

If the asset is part of a project, the Resource is added as a child of the Control Plan.
 - If the asset exists in OpenPages, the import process checks for updates, such as links to other projects and changes to the status of the asset.

When projects or assets change, the import process makes the following updates:

- If a project is deleted from Watson Knowledge Catalog or if it no longer contains classified assets, the Control Plan remains in OpenPages. The import process changes the Status field on the Control Plan object to **No Longer Private**.

- If an asset no longer matches the classifications that you configured for the import, the import process changes the Status field on the Resource object to **No Longer Private**.

If an asset is deleted from Watson Knowledge Catalog, the the import process changes the Status field on the Resource object to **Deleted**.

Note: The import process does not update names. If an asset is renamed in Watson Knowledge Catalog and you want to use the new name in OpenPages, manually delete the resource and then re-import it into OpenPages.

Installing IBM OpenPages Data Privacy Management

If you want to use IBM OpenPages Data Privacy Management (DPM), you must install it. Do this task if you are entitled to use DPM.

Installing DPM on IBM OpenPages for IBM Cloud Pak for Data

Before you begin

- You have IBM OpenPages for IBM Cloud Pak for Data 8.2.2 or later and you have an OpenPages instance.
- The ObjectManager tool is installed on a computer that has access to the cluster. See [“Installing tools and utilities \(IBM OpenPages with Watson\)”](#) on page 824.
- To use DPM, you must also have a Watson Knowledge Catalog instance on IBM Cloud Pak for Data.

Procedure

1. Download the IBM OpenPages Data Privacy Management package from Passport Advantage.
2. Locate the `DPM_WKC_8202_Loader_Files.zip` file. Put the file in a new directory called `dpm-8202` on the computer where ObjectManager is installed.
3. Expand the `DPM_WKC_8202_Loader_Files.zip` file.
4. Do steps 1-3 in [“Preparing the instance”](#) on page 46.
The instance is ready for a configuration change. One replica is running.
5. On the computer where the ObjectManager tool is installed, go to the `openpages-tools-client/bin` directory.
6. Run the following command.

```
./Run_DPM_WKC_full.sh <op_admin_user> <op_admin_password>
```

If you encounter any errors, review the log file, `ObjectManager.log`.

7. Do the steps in [“Backing up changes and implementing them across replicas”](#) on page 46.
8. Optional: Remove the `dpm-8202` directory that you created in step 2.

What to do next

Import a TLS/SSL certificate from Watson Knowledge Catalog. See [“Importing a certificate into the local trust store on IBM OpenPages for IBM Cloud Pak for Data”](#) on page 61.

Installing DPM on IBM OpenPages with Watson

Before you begin

- IBM OpenPages with Watson 8.2.0.2 or later is installed.
- To use DPM, you must also have a Watson Knowledge Catalog instance on IBM Cloud Pak for Data.

Procedure

1. Download the IBM OpenPages Data Privacy Management package from Passport Advantage.
2. Locate the `DPM_WKC_8202_Loader_Files.zip` file. Copy the file to the application server. Put the file in a new directory, for example `dpm-8202`.
3. Expand the `DPM_WKC_8202_Loader_Files.zip` file.
4. Open a command line.
If you are using Microsoft Windows, open a command prompt with the **Run as Administrator** option.
5. Run the following command:

Linux

```
./Run_DPM_WKC_full.sh <op_admin_user> <op_admin_password>
```

Windows

```
Run_DPM_WKC_full.bat <op_admin_user> <op_admin_password>
```

If you encounter any errors, review the log file, `ObjectManager.log`.

6. Optional: Remove the `dpm-8202` directory that you created in step 2.

What to do next

[“Importing a certificate for Watson Knowledge Catalog into the local trust store” on page 1035](#)

Importing a certificate for Watson Knowledge Catalog into the local trust store

If you are using OpenPages with Watson, you must import a certificate from Watson Knowledge Catalog to the local trust store. The certificate is needed to build a secure connection between the OpenPages with Watson application servers and the Watson Knowledge Catalog server.

About this task

Complete this task even if you do not use SSL/TLS.

Procedure

1. Get the certificate from Watson Knowledge Catalog and copy it to the OpenPages with Watson application server.
2. Log on to the OpenPages with Watson application server.
3. Import the certificate to WebSphere Liberty by running the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_NAME> -keystore  
<STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- `<CERTIFICATE_ALIAS>` is the alias of the certificate that you received from Watson Knowledge Catalog.
- `<CERTIFICATE_NAME>` is the file name of the certificate.
- `<STORE_PATH>` is the full path and file name of the trust store on the application server. For example: `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security/key.p12`
- `<STORE_PASSWORD>` is the password of the trust store on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

4. Restart the OpenPages with Watson services.
5. Repeat these steps on each application server.

Configuring the Watson Knowledge Catalog connector

Configure the import of Watson Knowledge Catalog metadata into IBM OpenPages with Watson.

Before you begin

- Get the following information:
 - Your Watson Knowledge Catalog credentials. You can use an API key and username or a password and username. The username must have access to the data that you want to import. If you want to use an API key, see [Generating an API key](#).
 - Your IBM Cloud Pak for Data URL.
 - The classifications in Watson Knowledge Catalog that you want to import.
- Import a TLS/SSL certificate from Watson Knowledge Catalog.

If you are using IBM OpenPages for IBM Cloud Pak for Data, see [“Importing a certificate into the local trust store on IBM OpenPages for IBM Cloud Pak for Data”](#) on page 61.

If you are using OpenPages with Watson, see [“Importing a certificate for Watson Knowledge Catalog into the local trust store ”](#) on page 1035.

About this task

To do this task, you need the following application permissions:

- **SOX > Administration > Scheduler**

Procedure

1. Log in to the Task Focused UI.
2. Click  > **Solution Configuration > Scheduler**.
3. Click the **Data Privacy WKC Import** job.
4. Click **Edit**.
5. Configure the connector:

- Enter your credentials.

If you want to use an API key, enter your Watson Knowledge Catalog API key and username, and then type undefined in the **Password** field.

If you want to use a password, enter your Watson Knowledge Catalog username and password, and then type undefined in the **API Key** field.

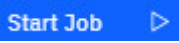
- Click **Base URL** and type your IBM Cloud Pak for Data URL.
- Verify the value in the **Parent Entity Path** field. The objects that are created during the import are created under this path. You can use the default or specify another path.
- Click **WKC Classifications** and type a comma-separated list of classifications. Assets with these classifications will be imported. The classification names must match the names in Watson Knowledge Catalog.

For example, Sensitive Personal Information, Personally Identifiable Information, Electronic Protected Health Information

- If you want to reload all data, click **Reload All** and set it to true. If you want to import only new data, set it to false.
- In the **Schedule** section, click **Edit**. Set the schedule for the import.

6. Click **Done**.

The connector is configured and the import is scheduled.

7. If you want to import data from Watson Knowledge Catalog now, click the checkbox next to the **Data Privacy WKC Import** job and then click .

What to do next

To see the progress of an import, go to  > **Solution Configuration** > **Scheduler**. click the **Data Privacy WKC Import** job, and then click the **Executions** tab. Click a process to view the log.

Chapter 37. Configuring IBM OpenPages Regulatory Compliance Management

You can configure IBM OpenPages Regulatory Compliance Management (RCM).

For example, you can import data from Ascent Reg Tech, Reg-Track, Thomson Reuters Regulatory Intelligence, or Wolters Kluwer. You can also configure the RCM Theme Deployer.

Ascent Connector

IBM OpenPages Regulatory Compliance Management (RCM) includes a connector for Ascent Reg Tech (Ascent).

The Ascent connector enables you to load Ascent regulatory library content directly into RCM as Mandate, Sub-Mandate, and Requirement objects.

Table 307. Ascent content categorization	
Ascent content that is categorized as a ...	Is loaded as a...
Section	Mandate
Rule	Sub-Mandate
Task	Requirement

During the data load, Sub-Mandates are associated to their parent Mandate objects. Also, Requirements are associated to their parent Sub-Mandate and to their grandparent Mandate through its Sub-Mandate association.

When regulators update or add content, Ascent provides updates through its feeds. The updates are then loaded into OpenPages by a scheduled job to update the regulatory library objects.

Note: To use the connector, you must meet the following prerequisites:

- You must have an Ascent subscription. Work with Ascent to set up a feed. For more information, contact Ascent.
- You must install the Ascent connector. For more information, contact IBM OpenPages Support.

When OpenPages imports regulatory feeds from Ascent, it does the following tasks:

- Creates an object for each new incoming Mandate, Sub-Mandate, or Requirement and adds them to your regulatory library under /Library/RCM/RegLibrary/AscentRegLibrary. The Content Source field on each object is set to Ascent. For Mandates, the field is OPSS-Mand:Content Source. For Sub-Mandates, the field is OPSS-SubMand:Content Source. For Requirements, the field is OPSS-Req:Content Source.
- Updates existing Mandates and Sub-Mandates with any incoming changes.
- If a Requirement changes, the existing requirement is replaced with a new, updated Requirement.

Importing a certificate for Ascent into the local trust store

You must import a certificate from Ascent Reg Tech (Ascent) to the local trust store. The certificate is needed to build a secure connection between the OpenPages with Watson application servers and the Ascent server.

About this task

Complete this task even if you do not use SSL/TLS.

Procedure

1. Get the certificate from Ascent and copy it to the OpenPages with Watson application server.
To get a certificate, contact Ascent.
2. Log on to the OpenPages with Watson application server.
3. Import the certificate to WebSphere Liberty by running the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_NAME> -keystore  
<STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- <CERTIFICATE_ALIAS> is the alias of the certificate that you received from Ascent.
- <CERTIFICATE_NAME> is the file name of the certificate.
- <STORE_PATH> is the full path and file name of the trust store on the application server. For example: <OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/key.p12
- <STORE_PASSWORD> is the password of the trust store on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

4. Restart the OpenPages with Watson services.
5. Repeat these steps on each application server.

Configuring the Ascent connector

Configure the import of Ascent Reg Tech (Ascent) data into OpenPages.

Before you begin

To connect to Ascent, you need all of the following items:

- A TLS/SSL certificate from Ascent. For more information, see [“Importing a certificate for Ascent into the local trust store”](#) on page 1039.
- Your API token and API profile ID from Ascent.

About this task

To do this task, you need the following application permissions:

- **SOX > Administration > Ascent Feed**
- **SOX > Administration > Scheduler**

By default, OpenPages imports new data and updates since the last import. You can change this default behavior by using the **Max Days to Get** option. For example, suppose you imported data 120 days ago and you now want to import data only for the previous 30 days. In this case, you can set **Max Days to Get** to 30.

You can also reload data. For more information, see [“Reloading Ascent data”](#) on page 1041.

Procedure

1. Log in to the Task Focused UI.
2. Click  > **Solution Configuration > Scheduler**.
3. Click the **Ascent** job.
4. Click **Edit**.
5. Configure the connector:

- Click **API Token** and enter your Ascent API token.
 - Verify the value in the **Base URL** field.
 - To change the maximum number of days' data to import, click **Max Days to Get**.
 - Click **Profile ID** and enter your Ascent profile ID.
 - In the **Schedule** section, click **Edit**. Set the schedule for the import from Ascent.
6. Click **Done**.
- The connector is configured and the import is scheduled.
7. If you want to import data from Ascent now, click the checkbox next to the **Ascent** job and then click .

What to do next

To see the progress of an import, go to  > **Solution Configuration** > **Scheduler**. click the **Ascent** job, and click the **Executions** tab. Click a process to view the log.

Reloading Ascent data

You can reload Ascent data.

By default, IBM OpenPages with Watson loads changes since the last import, up to the number of days specified by **Max Days to Get** in the job configuration.

However, you can change the default behavior by changing the following setting to `true`: **Solutions** > **RCM** > **Ascent** > **Load Old Feeds**. When **Load Old Feeds** is `true`, OpenPages imports all of the data that is available, including data that was imported previously, up to the **Max Days to Get**.

For example, suppose that the most recent import was 10 days ago and **Max Days to Get** is set to 30. If you want to import all data for the past 30 days, set **Load Old Feeds** to `true`. With this configuration, OpenPages loads data from the past 30 days, even though some of the data was loaded during the previous import.

You can access the **Load Old Feeds** setting from the Task Focused UI or the Standard UI. For more information, see [“Managing settings \(Task Focused UI\)” on page 597](#) or [“Modifying settings \(Standard UI\)” on page 598](#).

Changes to this setting take effect the next time that you import from Ascent.

Thomson Reuters Connector

IBM OpenPages Regulatory Compliance Management (RCM) includes a connector for Thomson Reuters Regulatory Intelligence (TRRI).

The Thomson Reuters connector enables you to load regulatory event feeds from Thomson Reuters into RCM. You can set up rules to process the incoming regulatory events automatically. Rules trigger workflows that are assigned to users based on the data points in the regulatory events or in the documents that are impacted by a regulatory change. The rules help you to assign tasks to users efficiently so that they can respond to and prepare for regulatory changes.

You can also import regulatory library objects from Thomson Reuters into RCM.

When OpenPages imports regulatory events, it does the following tasks:

- Checks if there is a taxonomy change.

If a new Thomson Reuters taxonomy file is found on the SFTP server, OpenPages does the following tasks:

- Updates the RCM-TRRI-Taxonomy field group's enumerated values
- Sends an email to the users who are set up as TRRI Administrators.

For more information, see [“Thomson Reuters taxonomy updates”](#) on page 1048.

- Checks if the taxonomy mapping file has changed. If a new taxonomy file is found, OpenPages uses the new mappings when it imports regulatory events. For more information about the taxonomy mapping file, see [“Mapping Thomson Reuters taxonomy values to OpenPages field values”](#) on page 1047.
- For regulatory events, OpenPages does the following steps:
 - Creates a TRRI Regulatory Event object for each new incoming regulatory event.
 - Checks the series ID of each incoming regulatory event and looks for a TRRI Regulatory Event Series object with the same series ID.

If OpenPages finds a match, OpenPages associates the regulatory event with the TRRI Regulatory Event Series.

If a TRRI Regulatory Event Series object does not exist for the series ID, OpenPages creates one and associates the regulatory event with the new TRRI Regulatory Event Series object.
 - Checks each of the incoming regulatory events for related documents. If the citation field on a regulatory event matches the citation field on a Mandate, Sub-Mandate, or Requirement in your regulatory library, OpenPages adds the Mandate, Sub-Mandate, or Requirement as a related object of the TRRI Regulatory Event.
 - Checks each of the incoming regulatory events against all rules that are enabled in the **TRRI Rules Engine**. If the regulatory event meets all the conditions of a rule, the rule is triggered. For more information, see [“Processing regulatory events by using rules”](#) on page 1060.
- For regulatory library objects, OpenPages does the following steps:
 - Creates an object for each new incoming Sub-Mandate and adds them to your regulatory library under `Library/RCM/RegLibrary/TRRIRegLibrary`. The `OPSS-SubMand:Content Source` field on each object is set to Thomson Reuters
 - Uses the Thomson Reuters API to identify Mandates that are associated with the incoming Sub-Mandates and creates the Mandate objects in OpenPages. The new Mandates are added to your regulatory library under `Library/RCM/RegLibrary/TRRIRegLibrary`. The Sub-Mandates are associated with their parent Mandate. In addition, the Thomson Reuters categorizations of the Sub-Mandates are rolled up to the parent Mandate and are included in the Mandate details.
 - Updates existing Sub-Mandates with any incoming changes.
 - Updates existing Mandates with any new Sub-Mandate associations and any new categorizations from the associated Sub-Mandates.
 - Sends an email to the owner of the impacted Sub-Mandates.

Preparing the SFTP server

Prepare the SFTP server where the Thomson Reuters data will be delivered.

Procedure

1. Create a directory to use with OpenPages. Or, choose an existing directory.

This is the directory where the feeds will be delivered. OpenPages will download the feeds from this directory.
2. Create a user for OpenPages on the SFTP server. Give the user read and write permissions on the directory where the feeds will be delivered.

The user needs Write permission because OpenPages creates a temporary file on the SFTP server in order to read the server's time. This file is used to keep track of which files are new and which are old, so that old files are not re-imported. OpenPages does not modify or delete existing files on the SFTP server.
3. Gather information.

You need the following information when you configure the Thomson Reuters import in OpenPages:

 - The fully qualified domain name (FQDN) or IP address of the SFTP server

Note: Depending on your network configuration, you might need to use the IP address instead of the FQDN.

- The username and password of the user that you created in step 2
- The port number of the SFTP server (the default port is 22)
- The directory where the Thomson Reuters feeds will be delivered

This is the directory that you created in step 1.

4. Make sure that all application servers (admin and non-admin) can connect to the SFTP server by using the information in step 3.

Tip: You do not need to sync the clock between the OpenPages application servers and the SFTP server.

Configuring the feeds

In Thomson Reuters Regulatory Intelligence (TRRI), choose the feeds that you want to import into IBM OpenPages with Watson.

About this task

You can import data from multiple feeds, but the feeds must be delivered to the same directory on the SFTP server.

Procedure

1. Set up Thomson Reuters Regulatory Intelligence to deliver feeds to the SFTP server that you prepared for OpenPages.

For more information, see [“Preparing the SFTP server” on page 1042](#).

For information about setting up Thomson Reuters Regulatory Intelligence, see the documentation that is provided with Thomson Reuters Regulatory Intelligence or contact your Thomson Reuters representative.

2. Choose the feeds that you want to import into OpenPages.
 - For each feed, use the same delivery location. OpenPages reads from only one SFTP server directory.
 - Enable the **Regulatory Event summaries only** option for each feed. OpenPages does not process source documents from Thomson Reuters Regulatory Intelligence.
3. Click **Settings > Taxonomy**, and then do the following steps:
 - a) Set the delivery location of the taxonomies to the same directory as the feeds that you set up in step 2.
 - b) Enable the **Send taxonomy files as they are updated** check box.

4. Make a note of the directory where the feeds and taxonomy files will be delivered.

You need this information when you configure the Thomson Reuters import in OpenPages.

Importing a certificate for Thomson Reuters into the local trust store

You must import a certificate from Thomson Reuters Regulatory Intelligence (TRRI) to the local trust store. The certificate is needed to build a secure connection between the OpenPages with Watson application servers and the Thomson Reuters Regulatory Intelligence server.

About this task

Complete this step even if you do not use SSL/TLS.

Procedure

1. Get a certificate from Thomson Reuters and copy it to the OpenPages with Watson application server.

To get a certificate, contact Thomson Reuters.

2. Log on to the OpenPages with Watson application server.
3. Import the certificate to WebSphere Liberty by running the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_NAME> -keystore  
<STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- <CERTIFICATE_ALIAS> is the alias of the certificate that you received from Thomson Reuters.
- <CERTIFICATE_NAME> is the file name of the certificate.
- <STORE_PATH> is the full path and file name of the trust store on the application server. For example: <OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/key.p12
- <STORE_PASSWORD> is the password of the trust store on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

4. Restart the OpenPages with Watson services.
5. Repeat these steps on each application server.

Configuring the Thomson Reuters import

Configure the import of Thomson Reuters Regulatory Intelligence data into IBM OpenPages with Watson.

Before you begin

- To connect to Thomson Reuters Regulatory Intelligence, you need all of the following items:
 - A TLS/SSL certificate from Thomson Reuters. For more information, see [“Importing a certificate for Thomson Reuters into the local trust store”](#) on page 1043.
 - Your API client ID and API client secret from Thomson Reuters Regulatory Intelligence.
- Prepare the SFTP server. For more information, see [“Preparing the SFTP server”](#) on page 1042.
- Configure the feeds in Thomson Reuters Regulatory Intelligence. For more information, see [“Configuring the feeds”](#) on page 1043.
- Before you import, ensure that System Admin Mode is disabled. To disable System Admin Mode, click  > **Disable System Admin Mode**.

About this task

To do this task, you need the **SOX > Administration > TRRI Feed** permission.

Procedure

1. Log in to the Task Focused UI.
2. Click  to open the Primary menu.
3. Click **Regulatory Compliance > TRRI Regulatory Events**.
4. Click .
5. Enter values in the following fields:
 - **API Client ID** and **API Client Secret**: Type the API client ID and secret that you received from Thomson Reuters.
 - **Host**: Type the fully qualified domain name (FQDN) or IP address of the SFTP server where the feeds are delivered.

- **Username and Password:** Type the user name and password that is used by OpenPages to access the SFTP server.
- **Directory:** Type the directory on the SFTP server where the feeds are delivered. For more information, see [“Directory path for Thomson Reuters imports” on page 1045](#).
- **Port:** Type the port number of the SFTP server (the default is 22).
- **Daily Scheduled Import:** If you want to schedule the import, select a time. OpenPages imports the data each day. This field is optional.

Select a time later than the time that your Thomson Reuters feeds are scheduled to be delivered. Keep in mind that it can take some time for the feeds to be delivered to the SFTP server.

For more information, see [“Daily schedule for Thomson Reuters imports” on page 1045](#).

- **TRRI Administrators:** Use this field to select the users to notify if the import has errors or if the Thomson Reuters taxonomy changes. This field is optional.
 - Select one or more of the following options:
 - **Process Regulatory Events:** Select this option to import regulatory events data.
 - **Process Regulatory Library Objects:** Select this option to import related documents.
6. Optional: If you want to customize how the Thomson Reuters taxonomy is mapped to OpenPages fields, see [“Thomson Reuters taxonomy mapping” on page 1046](#).
7. If you want to import data from Thomson Reuters now, click **Start Import**. Otherwise, click **Done**.

What to do next

To see the progress of an import, go to  > **Solution Configuration** > **Scheduler**. Click the **Thomson Reuters Regulatory Intelligence** job, and click the **Executions** tab. Click a process to view the log.

Directory path for Thomson Reuters imports

When you configure the import of Thomson Reuters data into IBM OpenPages with Watson you need to specify the directory on the SFTP server where the feeds are delivered.

You can use an absolute or a relative path.

The path is relative to the default directory of the SFTP user that OpenPages uses to access the SFTP server.

For example, suppose that you are using a Linux server, the default directory for OpenPages is `/home/data`, and the Thomson Reuters feeds are delivered to a subdirectory called `feeds`. You can specify the feeds directory by using either of the following paths:

- `/home/data/feeds`
- `feeds`

Important: If you type a leading forward slash (`/`), the meaning of the path is different. A leading forward slash indicates an absolute path relative to the root directory. So, in this example, `/feeds` is `/home/feeds`.

Tip: You can also use a period (`.`) to specify the user's default directory, in this example `.` is equivalent to `/home/data`.

If your SFTP server is using Microsoft Windows, use a backslash (`\`) when you type the path.

Daily schedule for Thomson Reuters imports

When you configure the import of Thomson Reuters data into IBM OpenPages with Watson, you can choose the hour each day to do the import.

You can choose an hour between 00:00 and 23:00. OpenPages uses the clock of the OpenPages application servers to determine the time window.

Choose a time that is later than the time when the Thomson Reuters feeds are scheduled to be delivered. It can take some time for the Thomson Reuters data to arrive on the SFTP server.

For example, suppose that you choose 13:00. At 1PM each day, OpenPages attempts to import the data on the SFTP server. If the import fails, OpenPages continues to attempt the import until 1:59PM.

If OpenPages is shut down at the time you chose, OpenPages tries again when the servers are restarted, if the time window hasn't passed.

For example, suppose that you schedule the import for 13:00. If the OpenPages servers are shut down at 11:00AM and then restarted at 1:30PM, OpenPages imports the Thomson Reuters data at 1:30PM. If the servers are restarted after 1:59PM, however, OpenPages does not import data until the next day at 1PM.

Reloading Thomson Reuters data

You can reload Thomson Reuters feeds.

By default, IBM OpenPages with Watson imports new feeds only. During an import, all files that existed before the previous import are ignored.

However, you can change the default behavior by changing the following setting to `true`: **Solutions > RCM > TRRI > Load Old Feeds**. When **Load Old Feeds** is `true`, OpenPages imports all of the feeds that are in the directory on the SFTP server. The change takes effect the next time that you import from Thomson Reuters:

You can access the **Load Old Feeds** setting from the Task Focused UI or the Standard UI. For more information, see [“Managing settings \(Task Focused UI\)” on page 597](#) or [“Modifying settings \(Standard UI\)” on page 598](#).

Thomson Reuters taxonomy mapping

You can map the Thomson Reuters taxonomy to field values in IBM OpenPages with Watson.

You map values by downloading, modifying, and then uploading the Thomson Reuters taxonomy mapping file. The mapping file is a CSV text file.

For example, the Thomson Reuters taxonomy includes theme names, but you might want to use different names for some or all of the themes. Suppose that the theme names that you want to use are in the RCM-Shared:Themes field. You can map the Thomson Reuters theme names to the values of the RCM-Shared:Themes field. The field that you use must be an enumerated string field. Add the RCM-Shared:Themes to the TRRI Regulatory Event object type and then modify the taxonomy mapping file.

	A	B	C	D	E	F	G	H	I
1844	TRRI	ContentType	I7438E580A9FE11	Secondary Sources Treatises					
1845	TRRI	Themes	IE5B7F470458211	Business Activities					
1846	TRRI	Themes	IE5C1B870458211	Business Activities Banking	RCM-Shared	Themes	BA-B		
1847	TRRI	Themes	IE5C22DA0458211	Business Activities Banking Commercial lending	RCM-Shared	Themes	BA-B-COMM-L		
1848	TRRI	Themes	IE5C254B0458211	Business Activities Banking Consumer credit	RCM-Shared	Themes	BA-B-CON-CR		
1849	TRRI	Themes	IE5C2A2D0458211	Business Activities Banking Electronic banking / transactions	RCM-Shared	Themes	BA-B-E-TR		
1850	TRRI	Themes	IE5B44230622211	Business Activities Banking Foreclosure	RCM-Shared	Themes	BA-B-F		
1851	TRRI	Themes	IE5C2C9E0458211	Business Activities Banking Foreign operations	RCM-Shared	Themes	BA-B-FO		
1852	TRRI	Themes	IE5C31800458211	Business Activities Banking Investment activities - Banking					
1853	TRRI	Themes	IE5C1DF80458211	Business Activities Banking Payment systems / negotiable instruments					
1854	TRRI	Themes	IE5C38D30458211	Business Activities Banking Public monies					
1855	TRRI	Themes	IE5C3B440458211	Business Activities Banking Real estate / mortgage lending					
1856	TRRI	Themes	IE5C40260458211	Business Activities Banking Repayment protection					
1857	TRRI	Themes	IE5C42970458211	Business Activities Banking Savings and deposits					

Figure 84. Example of mapping Thomson Reuters themes to field values in OpenPages

Notice that you do not need to map all Thomson Reuters values to field values in OpenPages. If you do not map all values in the OpenPages field to a Thomson Reuters value, however, those fields will not get values automatically when the Thomson Reuters data is imported.

You can map multiple Thomson Reuters values to the same OpenPages field value.

You can also map a single Thomson Reuters value to multiple OpenPages field values. For example, suppose that you want to map the Thomson Reuters value **Business Activities | Banking** to **BA** and **Banking** in OpenPages. Copy the **Business Activities | Banking** row. In one of the rows, type **BA** in column H. In the other **Business Activities | Banking** row, type **Banking** in column H.

Mapping Thomson Reuters taxonomy values to OpenPages field values

You can map values in the Thomson Reuters taxonomy to values in IBM OpenPages with Watson. You define the mappings by editing the taxonomy mapping file.

Before you begin

- Ensure that each field group that you want to use is associated with the TRRI Regulatory Event object type.
- Ensure that each field that you want to use is an enumerated string field. The values that you want to use in the mapping file must be available in the enumerated string field.

About this task

To do this task, you need the **SOX > Administration > TRRI Feed** permission.

Procedure

1. Log in to the Task Focused UI.
2. Click  to open the Primary menu.
3. Click **Regulatory Compliance > TRRI Regulatory Events**.
4. Click .
5. Click **Download the latest mapping file (.csv)** and save the file.
6. Create a backup of the `trri_taxonomy_map.csv` file.

7. Open the `trri_taxonomy_map.csv` file.

	A	B	C	D	E	F	G	H	I
1	Ve Vendo		Vendor Field	Vendor Value Id	Vendor Value	Group	Field	Value	
2		TRRI	Geography	ID4CB7E80459011	Africa				
3		TRRI	Geography	ID4CBA590459011	Africa Algeria				
4		TRRI	Geography	ID4CBF3B0459011	Africa Angola				
5		TRRI	Geography	ID4CC1AC0459011	Africa Benin				
6		TRRI	Geography	ID4CC68E0459011	Africa Botswana				
7		TRRI	Geography	ID4CCB700459011	Africa Burkina Faso				
8		TRRI	Geography	ID4CCDE10459011	Africa Burundi				
9		TRRI	Geography	ID4CD2C30459011	Africa Cameroon				
10		TRRI	Geography	ID4CD5340459011	Africa Cape Verde				
11		TRRI	Geography	ID4CD7A50459011	Africa Central African Republic				
12		TRRI	Geography	ID4CDC870459011	Africa Chad				
13		TRRI	Geography	ID4CDEF80459011	Africa Congo				
14		TRRI	Geography	ID4D0AEA0459011	Africa CÃ'te d'Ivoire				

Figure 85. Example of the taxonomy file in Microsoft Excel

8. In column E, locate the Thomson Reuters value that you want to map to a field value in OpenPages.

9. For each value that you want to map, enter the following information:

- In column F, type the field group.
- In column G, type the field name.
- In column H, type the field value.

The Thomson Reuters value in column E will be mapped to the OpenPages value in column H.

Note: Do not edit the values in columns A to E.

10. Save the file as a CSV text file.

11. Return to OpenPages.

12. On the **TRRI Regulatory Events** page, click .

13. Click **Upload**.

Results

The taxonomy mapping file is uploaded. The next time that you import data from Thomson Reuters, your taxonomy mappings are applied to the incoming regulatory events.

Thomson Reuters taxonomy updates

If you modified the taxonomy mapping file, you need to update it when the Thomson Reuters taxonomy changes.

When Thomson Reuters updates the taxonomy, it delivers a new taxonomy file to the SFTP server. IBM OpenPages with Watson checks for a new taxonomy file each time it imports data from Thomson Reuters. If OpenPages detects a new taxonomy file, it sends an email to the **TRRI Administrators**. The **TRRI Administrators** are configured when you configure the Thomson Reuters import. For more information, see [“Configuring the Thomson Reuters import” on page 1044](#).

Review the taxonomy changes that are listed in the email. Update the taxonomy mapping file manually to include the changes. You might also need to update the fields in OpenPages. For example, if Thomson Reuters adds a new theme to the taxonomy, you might need to add a new value to the field that you use for theme names. When the taxonomy mapping file is ready and the OpenPages fields are updated, upload the taxonomy mapping file.

Reg-Track Connector

IBM OpenPages Regulatory Compliance Management (RCM) includes a connector for Reg-Track.

The Reg-Track connector enables you to load regulatory events from Reg-Track into RCM. You can set up rules to process the incoming regulatory events automatically. Rules trigger workflows that are assigned to users based on the data points in the regulatory events. The rules help you to assign tasks to users efficiently so that they can respond to and prepare for regulatory changes.

Note: To use the connector, you must meet the following prerequisites:

- You must have a Reg-Track subscription. For more information, contact Reg-Track.
- You must install the Reg-Track connector. For more information, contact your IBM representative.

When OpenPages imports regulatory event feeds from Reg-Track, it does the following tasks:

- Checks if there are any changes to the Reg-Track taxonomy.

If changes are found, OpenPages does the following tasks:

- Updates the fields in the RCM-RegTrack-Taxonomy field group.
- Sends an email to the users who are set up as Reg-Track Administrators.

For more information, see [“Reg-Track taxonomy updates” on page 1054](#).

- Checks if the taxonomy mapping file has changed. If a new taxonomy mapping file is found, OpenPages uses the new mappings when it imports regulatory feeds. For more information about the taxonomy mapping file, see [“Mapping Reg-Track taxonomy values to OpenPages field values” on page 1052](#).
- For regulatory events, OpenPages does the following steps:

- Creates a Reg-Track Regulatory Event object for each new incoming regulatory event.
- Checks the Reg-Track Series ID of each incoming regulatory event and looks for a Reg-Track Regulatory Event Series object with the same series ID.

If OpenPages finds a match, OpenPages associates the regulatory event with the Reg-Track Regulatory Event Series.

If a Reg-Track Regulatory Event Series object does not exist for the series ID, OpenPages creates one and associates the regulatory event with the new Reg-Track Regulatory Event Series object.

- Checks each of the incoming regulatory events against all of the Reg-Track rules that are enabled in OpenPages. If the regulatory event meets the conditions of a rule, the rule is triggered. For more information, see [“Processing regulatory events by using rules” on page 1060](#).

Importing a certificate for Reg-Track into the local trust store

You must import a certificate from Reg-Track to the local trust store. The certificate is needed to build a secure connection between the OpenPages with Watson application servers and the Reg-Track server.

About this task

Complete this task even if you do not use SSL/TLS.

Procedure

1. Get the certificate from Reg-Track and copy it to the OpenPages with Watson application server.
To get a certificate, contact Reg-Track.
2. Log on to the OpenPages with Watson application server.
3. Import the certificate to WebSphere Liberty by running the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_NAME> -keystore  
<STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- <CERTIFICATE_ALIAS> is the alias of the certificate that you received from Reg-Track.
- <CERTIFICATE_NAME> is the file name of the certificate.
- <STORE_PATH> is the full path and file name of the trust store on the application server. For example: <OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/key.p12
- <STORE_PASSWORD> is the password of the trust store on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

4. Restart the OpenPages with Watson services.
5. Repeat these steps on each application server.

Configuring the Reg-Track connector

Configure the import of Reg-Track data into OpenPages.

Before you begin

To connect to Reg-Track, you need all of the following items:

- A TLS/SSL certificate from Reg-Track. For more information, see [“Importing a certificate for Reg-Track into the local trust store” on page 1049](#).
- The Reg-Track API URL.
- Your Reg-Track API client key.
- Your Reg-Track API client secret.
- Your Reg-Track API token.

Before you import, ensure that System Admin Mode is disabled. To disable System Admin Mode, click  > **Disable System Admin Mode**.

About this task

To do this task, you need the **SOX > Administration > RegTrack Feed** application permission.

By default, OpenPages imports new data and updates since the last import. You can change this default behavior. For more information, see [“Data import settings for Reg-Track feeds” on page 1051](#).

Note: When you run the import for the first time, OpenPages imports data for the past 7 days by default.

Procedure

1. Log in to the Task Focused UI.
2. Click  to open the Primary menu.
3. Click **Regulatory Compliance > Reg-Track Regulatory Events**.
4. Click .
5. Configure the import:
 - Type the API parameters that were provided to you by Reg-Track.
 - **Daily Scheduled Import:** If you want to schedule the import, select a time. OpenPages imports the data each day. This field is optional.

Select a time that is later than when Reg-Track delivers its feeds. Contact Reg-Track for information about when feeds are delivered.
 - **Reg-Track Administrators:** Use this field to select the users to notify if the import has errors or if the Reg-Track taxonomy changes. This field is optional.

- **Process Regulatory Events:** Click to map incoming regulatory events to Reg-Track Regulatory Events in OpenPages. If not selected, OpenPages checks for an updated taxonomy file only.
6. Optional: If you want to customize how the Reg-Track taxonomy is mapped to OpenPages fields, see [“Reg-Track taxonomy mapping” on page 1051](#).
 7. If you want to import data from Reg-Track now, click **Start Import**. Otherwise, click **Done**.

What to do next

To see the progress of an import, go to  > **Solution Configuration** > **Scheduler**. click the **Reg Track** job, and click the **Executions** tab. Click a process to view the log.

Data import settings for Reg-Track feeds

By default, OpenPages imports new data only. You can change this default behavior.

You can use the following settings:

- **Solutions > RCM > WK > Load Old Feeds**

When **Load Old Feeds** is `false`, OpenPages imports only new data. The maximum number of days to import is specified in the **Max Days To Get** setting.

When **Load Old Feeds** is `true`, OpenPages loads the data from previous days, regardless of whether the data was imported previously. You can import data from a maximum of 7 days ago. The maximum number of days to import is specified in the **Max Days To Get** setting.

- **Solutions > RCM > WK > Max Days To Get**

This setting specifies the maximum number of days to import. The default value is 5. The maximum number of days that you can import is 7.

Changes to these settings take effect the next time that you import from Reg-Track.

You can access these settings from the Task Focused UI or the Standard UI. For more information, see [“Managing settings \(Task Focused UI\)” on page 597](#) or [“Modifying settings \(Standard UI\)” on page 598](#).

Example 1: Setting the maximum number of days of new data to import

Suppose you want to load any new data from the past 5 days.

In this case, set **Load Old Feeds** to `false` and set **Max Days To Get** to 5. With this configuration, OpenPages loads new data up to a maximum of 5 days ago. If the most recent import occurred 2 days ago, OpenPages loads the data only for the last 2 days. If the most recent import occurred 4 days ago, OpenPages loads the data only for the last 4 days.

Example 2: Reloading data

Suppose that the most recent import was 3 days ago but you want to get all data from the past 7 days.

In this case, set **Load Old Feeds** to `true` and set **Max Days To Get** to 7. With this configuration, OpenPages loads data from the past 7 days, even though some of the data was loaded during the previous import.

Reg-Track taxonomy mapping

You can map the Reg-Track taxonomy to field values in IBM OpenPages with Watson.

You map values by downloading, modifying, and then uploading the Reg-Track taxonomy mapping file. The mapping file is a CSV text file.

For example, the Reg-Track taxonomy includes countries and regions. You might want to group the countries into different regions or create additional regions. Suppose that the values that you want to use are in the RCM-Shared:CustomGeo field. You can map the Reg-Track countries to the values of

the RCM-Shared:CustomGeo field. The field that you use must be an enumerated string field. Add the RCM-Shared:CustomGeo field to the Reg-Track Regulatory Event object type and then modify the taxonomy mapping file.

Note: The following figure shows a excerpt of rows from the taxonomy mapping file to illustrate the example. This figure is not a representation of the entire file.

	A	B	C	D	E	F	G	H
3	Version	Vendor	Vendor Field	Vendor Value Id	Vendor Value	Group	Field	Value
4		Reg-Track	Countries	118	Antigua	RCM-Shared	CustomGeo	Caribbean
5		Reg-Track	Countries	121	Aruba	RCM-Shared	CustomGeo	Caribbean
6		Reg-Track	Countries	79	Bahamas	RCM-Shared	CustomGeo	Caribbean
7		Reg-Track	Countries	75	Cayman Islands	RCM-Shared	CustomGeo	Caribbean
8		Reg-Track	Countries	181	Jamaica	RCM-Shared	CustomGeo	Caribbean
9		Reg-Track	Countries	153	Trinidad and Tobago	RCM-Shared	CustomGeo	Caribbean
10		Reg-Track	Countries	150	US Virgin Islands	RCM-Shared	CustomGeo	Caribbean
11		Reg-Track	Countries	36	Yemen			
12		Reg-Track	Countries	59	Zimbabwe			

Figure 86. Example of mapping Reg-Track countries to a field value in OpenPages

You do not need to map all Reg-Track values to field values in OpenPages. If you do not map all values in the OpenPages fields to a Reg-Track value, those fields will not get values automatically when the Reg-Track data is imported.

You can map multiple Reg-Track values to the same OpenPages field value.

You can also map a single Reg-Track value to multiple OpenPages field values. For example, suppose that you want to map the Reg-Track value ABS to Derivatives and Asset Backed Securities in OpenPages. Copy the ABS row. In one of the rows, type Derivatives in column H. In the other ABS row, type Asset Backed Securities in column H.

Mapping Reg-Track taxonomy values to OpenPages field values

You can map values in the Reg-Track taxonomy to values in IBM OpenPages with Watson. You define the mappings by editing the taxonomy mapping file.

Before you begin

- Each field group that you want to use is associated with the Reg-Track Regulatory Event object type.
- Each field that you want to use is an enumerated string field. The values that you want to use in the mapping file must be available in the enumerated string field.

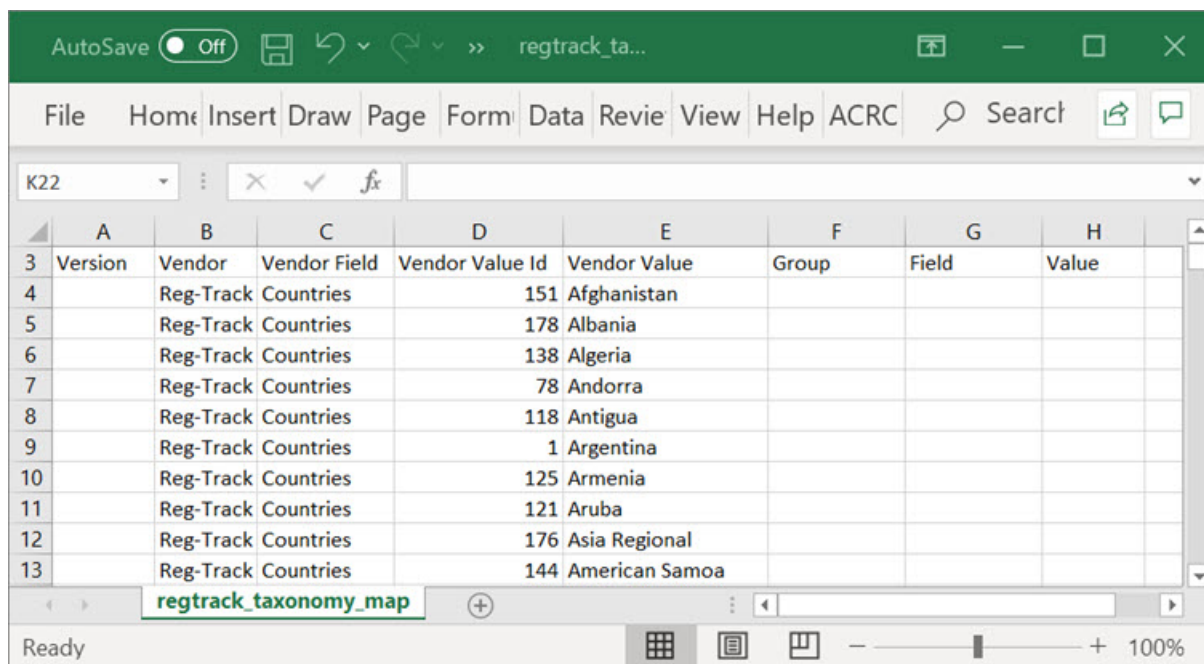
About this task

To do this task, you need the **SOX > Administration > RegTrack Feed** permission.

When you edit the taxonomy mapping file, use a text editor that supports UTF-8. Multibyte characters are not supported in the taxonomy mapping file.

Procedure

1. Log in to the Task Focused UI.
2. Click  to open the Primary menu.
3. Click **Regulatory Compliance > Reg-Track Regulatory Events**.
4. Click .
5. Click **Download the latest mapping file (.csv)** and save the file.
6. Create a backup of the `regtrack_taxonomy_map.csv` file.
7. Open the `regtrack_taxonomy_map.csv` file.



	A	B	C	D	E	F	G	H
3	Version	Vendor	Vendor Field	Vendor Value Id	Vendor Value	Group	Field	Value
4		Reg-Track	Countries	151	Afghanistan			
5		Reg-Track	Countries	178	Albania			
6		Reg-Track	Countries	138	Algeria			
7		Reg-Track	Countries	78	Andorra			
8		Reg-Track	Countries	118	Antigua			
9		Reg-Track	Countries	1	Argentina			
10		Reg-Track	Countries	125	Armenia			
11		Reg-Track	Countries	121	Aruba			
12		Reg-Track	Countries	176	Asia Regional			
13		Reg-Track	Countries	144	American Samoa			

Figure 87. Example of the taxonomy file in Microsoft Excel

8. In column E, locate the Reg-Track value that you want to map to a field value in OpenPages.
9. For each value that you want to map, enter the following information:
 - In column F, type the field group.
 - In column G, type the field name.
 - In column H, type the field value.

The Reg-Track value in column E will be mapped to the value in column H.

Note: Do not edit the values in columns A to E.

10. Save the file as a CSV text file.
11. Return to OpenPages.
12. On the **Reg-Track Regulatory Events** page, click .
13. Click **Upload**.

Results

The taxonomy mapping file is uploaded. The next time that you import data from Reg-Track, your taxonomy mappings are applied to the incoming regulatory events.

Reg-Track taxonomy updates

If you modified the taxonomy mapping file, you need to update it when the Reg-Track taxonomy changes.

IBM OpenPages with Watson checks for taxonomy changes each time it imports data from Reg-Track. If OpenPages detects changes to the taxonomy, it updates the fields in the RCM-RegTrack-Taxonomy field group and then sends an email to the **Reg-Track Administrators**. The **Reg-Track Administrators** are configured when you configure the Reg-Track connector. For more information, see [“Configuring the Reg-Track connector”](#) on page 1050.

Review the taxonomy changes that are listed in the email. Update the taxonomy mapping file manually to include the changes. You might also need to update the fields in OpenPages. For example, if Reg-Track adds a new product type to the taxonomy, you might need to add a new value to the field that you use for product types. When the taxonomy mapping file is ready and the OpenPages fields are updated, upload the taxonomy mapping file.

Wolters Kluwer Connector

IBM OpenPages Regulatory Compliance Management (RCM) includes a connector for Wolters Kluwer (WK).

The Wolters Kluwer connector enables you to load regulatory feeds from Wolters Kluwer into RCM. You can set up rules to process the incoming regulatory data automatically. Rules trigger workflows that are assigned to users based on the data points in the regulatory events or in the documents that are impacted by a regulatory change. The rules help you to assign tasks to users efficiently so that they can respond to and prepare for regulatory changes.

Note: To use the connector, you must meet the following prerequisites:

- You must have a Wolters Kluwer license. For more information, contact Wolters Kluwer.
- You must install the Wolters Kluwer connector. For more information, contact IBM OpenPages Support.

When OpenPages imports regulatory feeds from Wolters Kluwer, it does the following tasks:

- Checks if there are any changes to the Wolters Kluwer taxonomy.

If changes are found, OpenPages does the following tasks:

- Updates the fields in the RCM-WK-Taxonomy field group.
- Sends an email to the users who are set up as Wolters Kluwer Administrators.

For more information, see [“Wolters Kluwer taxonomy updates”](#) on page 1059.

- Checks if the taxonomy mapping file has changed. If a new taxonomy mapping file is found, OpenPages uses the new mappings when it imports regulatory feeds. For more information about the taxonomy mapping file, see [“Mapping Wolters Kluwer taxonomy values to OpenPages field values”](#) on page 1058.
- For regulatory events, OpenPages does the following steps:
 - Creates a WK Regulatory Event object for each new incoming regulatory event.
 - Checks each of the incoming regulatory events for related documents in your regulatory library. If the citation field on a regulatory event matches the citation field on a Mandate, Sub-Mandate, or Requirement, OpenPages adds the Mandate, Sub-Mandate, or Requirement as a related object of the WK Regulatory Event.
 - Checks each of the incoming regulatory events against all of the Wolters Kluwer rules that are enabled in OpenPages. If the regulatory event meets the conditions of a rule, the rule is triggered. For more information, see [“Processing regulatory events by using rules”](#) on page 1060.
- For regulatory library objects, OpenPages does the following steps:
 - Creates an object for each new incoming Mandate or Sub-Mandate and adds them to your regulatory library under `Library/RCM/RegLibrary/WKRegLibrary`. The `Content Source` field on each object is set to Wolters Kluwer. For Mandates, the field is `OPSS-Mand:Content Source`. For Sub-Mandates, the field is `OPSS-SubMand:Content Source`.

- Updates existing Mandates and Sub-Mandates with any incoming changes.
- Sends an email to the owner of the impacted Mandates and Sub-Mandates.

Importing a certificate from Wolters Kluwer to the local trust store

You must import a certificate from Wolters Kluwer to the local trust store. The certificate is needed to build a secure connection between the OpenPages with Watson application servers and the Wolters Kluwer server.

About this task

Complete this task even if you do not use SSL/TLS.

Procedure

1. Get the certificate from Wolters Kluwer and copy it to the OpenPages with Watson application server..
To get a certificate, contact Wolters Kluwer.
2. Log on to the OpenPages with Watson application server.
3. Import the certificate to WebSphere Liberty by running the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_NAME> -keystore <STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- <CERTIFICATE_ALIAS> is the alias of the certificate that you received from Wolters Kluwer.
- <CERTIFICATE_NAME> is the file name of the certificate.
- <STORE_PATH> is the full path and file name of the trust store on the application server. For example: <OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/key.p12
- <STORE_PASSWORD> is the password of the trust store on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

4. Restart the OpenPages with Watson services.
5. Repeat these steps on each application server.

Configuring the Wolters Kluwer import

Configure the import of Wolters Kluwer data into IBM OpenPages with Watson.

Before you begin

To connect to Wolters Kluwer, you need all of the following items:

- A TLS/SSL certificate from Wolters Kluwer. For more information, see [“Importing a certificate from Wolters Kluwer to the local trust store”](#) on page 1055.
- Get the following URLs and Feed Manager API parameters from Wolters Kluwer:
 - The authentication URL for the Wolters Kluwer API
 - The API URL for regulatory change updates.
 - The API URL for regulatory library updates.
 - Your Wolters Kluwer Client ID.
 - Your Wolters Kluwer Client Secret.
 - Your username and password for the Wolters Kluwer API.
 - The docSourceName parameter.

- The `sourceSystemCode` parameter.
- The `transformCode` parameter.

Before you import, ensure that System Admin Mode is disabled. To disable System Admin Mode, click  > **Disable System Admin Mode**.

About this task

To do this task, you need the **SOX > Administration > WK Feed** application permission.

By default, OpenPages imports new data only, and only for the past five days. You can change this default behavior. For more information, see [“Data import settings for Wolters Kluwer feeds” on page 1056](#).

Procedure

1. Log in to the Task Focused UI.
2. Click  to open the Primary menu.
3. Click **Regulatory Compliance > WK Regulatory Events**.
4. Click .
5. Configure the import:
 - Type the URLs and API parameters that were provided to you by Wolters Kluwer.
 - **Daily Scheduled Import:** If you want to schedule the import, select a time. OpenPages imports the data each day. This field is optional.

Select a time that is later than when Wolters Kluwer delivers its feeds. Contact Wolters Kluwer for information about when feeds are delivered.
 - **Wolters Kluwer Administrators:** Use this field to select the users to notify if the import has errors or if the Wolters Kluwer taxonomy changes. This field is optional.
 - **Process Regulatory Events:** Click to map Wolters Kluwer regulatory events to WK Regulatory Events in OpenPages..
 - **Process Regulatory Library Objects:** Click to map Wolters Kluwer library objects to Mandates, Sub-Mandates, and Requirements in OpenPages.
6. Optional: If you want to customize how the Wolters Kluwer taxonomy is mapped to OpenPages fields, see [“Wolters Kluwer taxonomy mapping” on page 1057](#).
7. If you want to import data from Wolters Kluwer now, click **Start Import**. Otherwise, click **Done**.

What to do next

To see the progress of an import, go to  > **Solution Configuration > Scheduler**. click the **Wolters Kluwer** job, and click the **Executions** tab. Click a process to view the log.

Data import settings for Wolters Kluwer feeds

By default, OpenPages imports new data only, and only for the past 5 days. You can change this default behavior.

You can use the following settings:

• **Solutions > RCM > WK > Load Old Feeds**

When **Load Old Feeds** is `false`, OpenPages imports only new data. The maximum number of days to import is specified in the **Max Days To Get** setting.

When **Load Old Feeds** is `true`, OpenPages loads the data from previous days, regardless of whether the data was imported previously. The maximum number of days to import is specified in the **Max Days To Get** setting.

- **Solutions > RCM > WK > Max Days To Get**

This setting specifies the maximum number of days to import. The default value is 5.

Changes to these settings take effect the next time that you import from Wolters Kluwer.

You can access these settings from the Task Focused UI or the Standard UI. For more information, see [“Managing settings \(Task Focused UI\)”](#) on page 597 or [“Modifying settings \(Standard UI\)”](#) on page 598.

Example 1: Setting the maximum number of days of new data to import

Suppose the last Wolters Kluwer import occurred more than 5 days ago. You want to load any new data from the past 10 days.

In this case, set **Load Old Feeds** to `false` and set **Max Days To Get** to 10. With this configuration, OpenPages loads new data up to a maximum of 10 days ago. If the most recent import occurred 6 days ago, OpenPages loads the data only for the last 6 days. If the most recent import occurred 18 days ago, OpenPages loads the data only for the last 10 days.

Example 2: Reloading data

Suppose that the most recent import was 5 days ago but you want to get all data from the past 10 days.

In this case, set **Load Old Feeds** to `true` and set **Max Days To Get** to 10. With this configuration, OpenPages loads data from the past 10 days, even though some of the data was loaded during the previous import.

Wolters Kluwer taxonomy mapping

You can map the Wolters Kluwer taxonomy to field values in IBM OpenPages with Watson.

You map values by downloading, modifying, and then uploading the Wolters Kluwer taxonomy mapping file. The mapping file is a CSV text file.

For example, the Wolters Kluwer taxonomy includes jurisdictions, but you might want to use different groupings for some or all of the jurisdictions. Suppose that the values that you want to use are in the `RCM-Shared:CustomGeo` field. You can map the Wolters Kluwer jurisdictions to the values of the `RCM-Shared:CustomGeo` field. The field that you use must be an enumerated string field. Add the `RCM-Shared:CustomGeo` field to the WK Regulatory Event object type and then modify the taxonomy mapping file.

	A	B	C	D	E	F	G	H	I
8		WK	Jurisdiction	WKFS-JUR-0000233	Eastern Asia South Korea Nepal				
9		WK	Jurisdiction	WKFS-JUR-0000234	Eastern Asia South Korea Pakistan				
10		WK	Jurisdiction	WKFS-JUR-0000235	Eastern Asia South Korea Sri Lanka				
11		WK	Jurisdiction	WKFS-JUR-0000279	North America Canada Alberta	RCM-Shared	CustomGeo	Canada-West	
12		WK	Jurisdiction	WKFS-JUR-0000280	North America Canada British Columbia	RCM-Shared	CustomGeo	Canada-West	
13		WK	Jurisdiction	WKFS-JUR-0000281	North America Canada Manitoba	RCM-Shared	CustomGeo	Canada-West	
14		WK	Jurisdiction	WKFS-JUR-0000283	North America Canada New Brunswick				
15		WK	Jurisdiction	WKFS-JUR-0000282	North America Canada Newfoundland & Labrador				
16		WK	Jurisdiction	WKFS-JUR-0000284	North America Canada Northwest Territories				
17		WK	Jurisdiction	WKFS-JUR-0000291	North America Canada Nova Scotia				
18		WK	Jurisdiction	WKFS-JUR-0000285	North America Canada Nunavut				
19		WK	Jurisdiction	WKFS-JUR-0000286	North America Canada Ontario				
20		WK	Jurisdiction	WKFS-JUR-0000287	North America Canada Prince Edward Island				

Figure 88. Example of mapping Wolters Kluwer jurisdictions to field values in OpenPages

Notice that you do not need to map all Wolters Kluwer values to field values in OpenPages. If you do not map all values in the OpenPages fields to a Wolters Kluwer value, those fields will not get values automatically when the Wolters Kluwer data is imported.

You can map multiple Wolters Kluwer values to the same OpenPages field value.

You can also map a single Wolters Kluwer value to multiple OpenPages field values. For example, suppose that you want to map the Wolters Kluwer value Audit Practice Bulletins to Audit Practices and Bulletins in OpenPages. Copy the Audit Practice Bulletins row. In one of the rows, type Audit Practices in column H. In the other Audit Practice Bulletins row, type Bulletins in column H.

Mapping Wolters Kluwer taxonomy values to OpenPages field values

You can map values in the Wolters Kluwer taxonomy to values in IBM OpenPages with Watson. You define the mappings by editing the taxonomy mapping file.

Before you begin

- Each field group that you want to use is associated with the WK Regulatory Event object type.
- Each field that you want to use is an enumerated string field. The values that you want to use in the mapping file must be available in the enumerated string field.

About this task

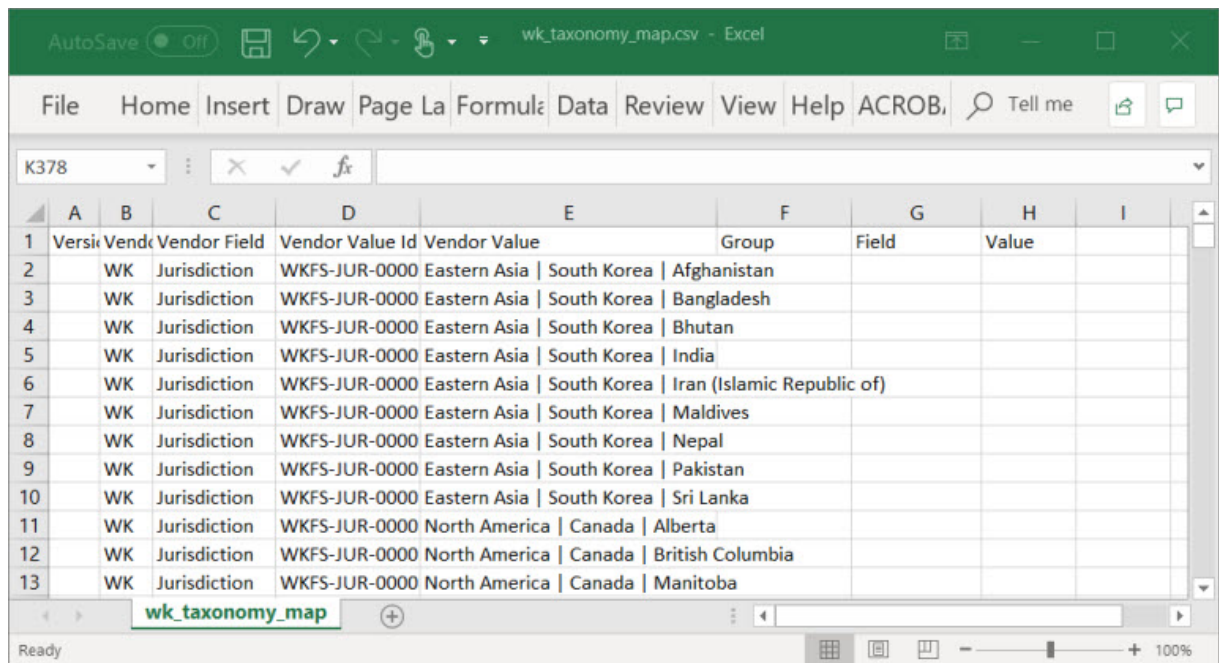
To do this task, you need the **SOX > Administration > WK Feed** permission.

When you edit the taxonomy mapping file, use a text editor that supports UTF-8. Multibyte characters are not supported in the taxonomy mapping file.

Procedure

1. Log in to the Task Focused UI.
2. Click  to open the Primary menu.
3. Click **Regulatory Compliance > WK Regulatory Events**.

4. Click .
5. Click **Download the latest mapping file (.csv)** and save the file.
6. Create a backup of the wk_taxonomy_map.csv file.
7. Open the wk_taxonomy_map.csv file.



	A	B	C	D	E	F	G	H	I
1	Vendor	Vendor Field	Vendor Value Id	Vendor Value	Group	Field	Value		
2	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia South Korea	Afghanistan				
3	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia South Korea	Bangladesh				
4	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia South Korea	Bhutan				
5	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia South Korea	India				
6	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia South Korea	Iran (Islamic Republic of)				
7	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia South Korea	Maldives				
8	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia South Korea	Nepal				
9	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia South Korea	Pakistan				
10	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia South Korea	Sri Lanka				
11	WK	Jurisdiction	WKFS-JUR-0000	North America Canada	Alberta				
12	WK	Jurisdiction	WKFS-JUR-0000	North America Canada	British Columbia				
13	WK	Jurisdiction	WKFS-JUR-0000	North America Canada	Manitoba				

Figure 89. Example of the taxonomy file in Microsoft Excel

8. In column E, locate the Wolters Kluwer value that you want to map to a field value in OpenPages.
9. For each value that you want to map, enter the following information:
 - In column F, type the field group.
 - In column G, type the field name.
 - In column H, type the field value.

The Wolters Kluwer value in column E will be mapped to the value in column H.

Note: Do not edit the values in columns A to E.

10. Save the file as a CSV text file.
11. Return to OpenPages.
12. On the **WK Regulatory Events** page, click .
13. Click **Upload**.

Results

The taxonomy mapping file is uploaded. The next time that you import data from Wolters Kluwer, your taxonomy mappings are applied to the incoming regulatory events.

Wolters Kluwer taxonomy updates

If you modified the taxonomy mapping file, you need to update it when the Wolters Kluwer taxonomy changes.

IBM OpenPages with Watson checks for taxonomy changes each time it imports data from Wolters Kluwer. If OpenPages detects changes to the taxonomy, it updates the fields in the RCM-WK-Taxonomy field group and then sends an email to the **Wolters Kluwer Administrators**. The **Wolters Kluwer Administrators** are configured when you configure the Wolters Kluwer import. For more information, see [“Configuring the Wolters Kluwer import” on page 1055](#).

Review the taxonomy changes that are listed in the email. Update the taxonomy mapping file manually to include the changes. You might also need to update the fields in OpenPages. For example, if Wolters Kluwer adds a new document type to the taxonomy, you might need to add a new value to the field that you use for document type names. When the taxonomy mapping file is ready and the OpenPages fields are updated, upload the taxonomy mapping file.

Processing regulatory events by using rules

You can process incoming regulatory events from Thomson Reuters Regulatory Intelligence or Wolters Kluwer by using rules.

About this task

You use rules to trigger automated workflows. An automated workflow has only a start stage and an end stage. OpenPages provides sample automated workflows. You can also create your own. When you create a workflow, enable the **Automated** option. The workflow is then available to use in rules.

OpenPages provides sample rules, which you can use or modify to meet your requirements. The sample rules are disabled by default. You can also create your own rules.

When a regulatory event is created, it's evaluated against all the rules that are enabled. For each rule, if its conditions are met, the automated workflow that is configured in the rule is started. A regulatory event can trigger more than one rule. The assignees and criticality are passed to the workflow as process variables. The workflow can use these parameters in values or regular expressions.

Note: Rules in the Rules Engine are triggered only as a result of a Thomson Reuters Regulatory Intelligence or Wolters Kluwer import.

Procedure

1. Learn about rules.
For example, look at the sample rules.
2. Create automated workflows to use in rules.
For more information, see [“Target actions in rules” on page 1062](#).
3. Create rules.
For more information, see [“Creating rules” on page 1060](#).
You can also edit rules, copy rules, delete rules, and enable or disable rules.

Creating rules

Create rules to route incoming Regulatory Events to users and groups.

About this task

To do this task, you need the **SOX > Administration > Rules Engine** permission.

Procedure

1. Log in to the Task Focused UI.
2. Click  to open the Primary menu.
3. Do one of the following steps:
 - If you are using Thomson Reuters Regulatory Intelligence, click **Regulatory Compliance > TRRI Regulatory Events** and then click **TRRI Rules Engine**.
 - If you are using Wolters Kluwer, click **Regulatory Compliance > WK Regulatory Events** and then click **Wolters Kluwer Rules Engine**.
4. Click **Add New**.

Note: You can also create a rule by copying an existing rule. See [“Copying a rule” on page 1063](#).

5. Type a **Name** for the rule.

6. Add one or more conditions.

When a regulatory event meets the conditions in a rule, the target action is triggered.

For more information, see [“Conditions in rules” on page 1061](#).

7. Select a **Target Action**.

Each action in the list is an automated workflow. When the conditions of the rule are all true, the automated workflow is started.

For more information, see [“Target actions in rules” on page 1062](#).

8. Select one or more **Users and Groups** to assign to the workflow.

9. Optional: Select a **Criticality**.

10. Click **Done**.

Tip: To delete a rule, click its check box and then click **Delete**. You can also disable a rule. See [“Enabling and disabling rules” on page 1064](#).

Conditions in rules

You can add one or more conditions to a rule. For each condition you build a comparison statement with two fields and an operator.

In **Compare** you choose the first field in the comparison statement.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is (or is not) a specified user or is (or is not) in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

In **Using** you choose an operator. The list of operators depends on the first field's field type.

In **To** you choose the second field in the comparison statement:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**.

- **An expression**

Enter a single field or variable from the list in [“Using variables, functions, and fields” on page 503](#). All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like `Evidence_[$Parent:SOXRisk/System Fields:Name$].pdf` if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can optionally add **Filter By** conditions.

Note: An object's system comment field (System Fields:Comment) cannot be used in a field comparison in a condition.

By default, all conditions must be met for the workflow in the **Target Action** field to start. However, you can override this default behavior by defining advanced logic to combine the conditions in a specific way. To override the default behavior, set **Advanced Logic** to true. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses. The order of operations is:

1. ()
2. NOT
3. AND
4. OR

For example, if you define three conditions, the default logic is that the target action is triggered if all three conditions are met: 1 and 2 and 3. However, if you define advanced logic, you can use the condition numbers together with the operators and, or, not, and parentheses:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

Target actions in rules

When you create a rule, you specify a target action. The target action is the automated workflow that is triggered when the conditions in the rule are true.

Each target action in the **Target Action** list is an automated workflow. You can add target actions to the list by creating automated workflows.

An automated workflow has only two stages: a start stage and end stage. In the workflow properties, **Automated** is set to **True**. The Send Email Notification workflow is an example of an automated workflow. For more information about workflows, see [Chapter 15, “Configuring GRC Workflow,” on page 495](#).

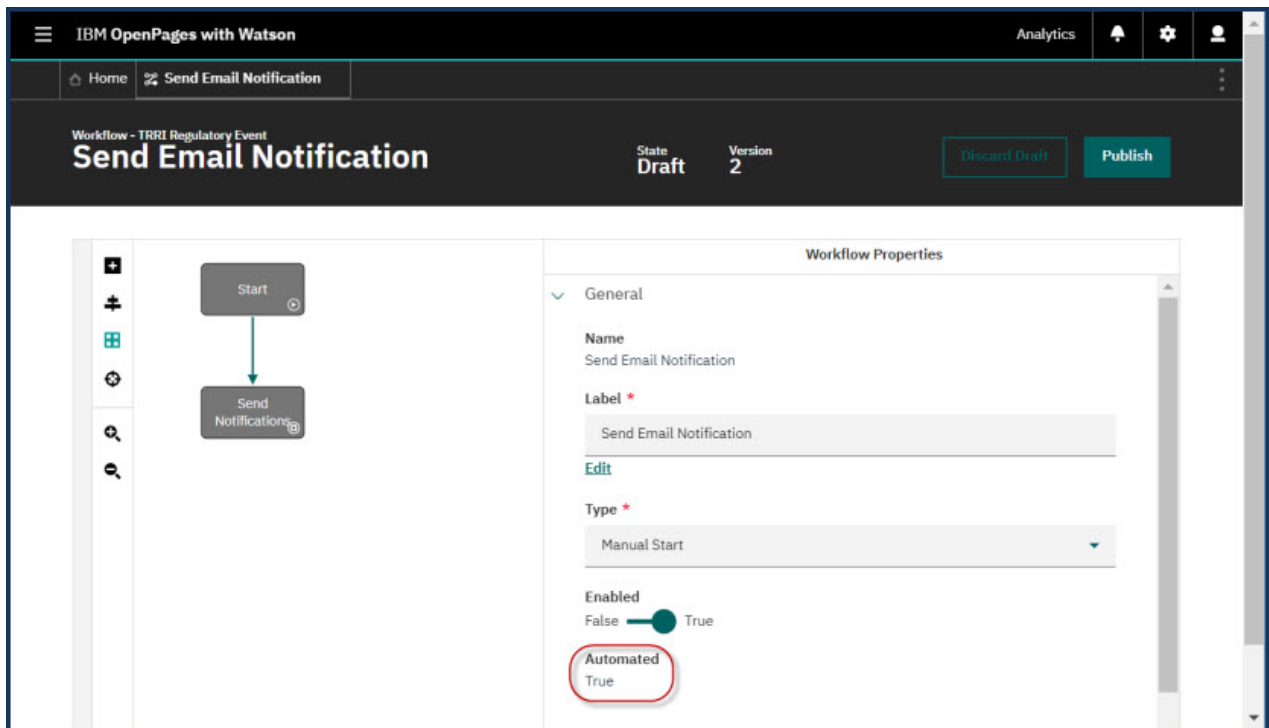


Figure 90. Send Email Notification sample workflow

Copying a rule

You can create a rule by copying an existing rule and then changing its properties.

About this task

To do this task, you need the **SOX > Administration > Rules Engine** permission.

Procedure

1. Log in to the Task Focused UI.
2. Click  to open the Primary menu.
3. Do one of the following steps:
 - If you are using Thomson Reuters Regulatory Intelligence, click **Regulatory Compliance > TRRI Regulatory Events** and then click **TRRI Rules Engine**.
 - If you are using Wolters Kluwer, click **Regulatory Compliance > WK Regulatory Events** and then click **Wolters Kluwer Rules Engine**.
4. Select the rules that you want to enable or disable by clicking its check box in the first column.
5. Click **Copy**.
6. Type a **Name** for the rule.
7. Edit the rule definition.

For more information, see [“Conditions in rules”](#) on page 1061 and [“Target actions in rules”](#) on page 1062.
8. Click **Done**.

Enabling and disabling rules

Enable a rule to make it active.

About this task

When a rule is enabled, it is used to process incoming Regulatory Events. When you create a new rule, it is enabled by default.

When a rule is disabled, it is not used but it is still available in the **Rules Engine**.

To do this task, you need the **SOX > Administration > Rules Engine** permission.

Procedure

1. Log in to the Task Focused UI.
2. Click  to open the Primary menu.
3. Do one of the following steps:
 - If you are using Thomson Reuters Regulatory Intelligence, click **Regulatory Compliance > TRRI Regulatory Events** and then click **TRRI Rules Engine**.
 - If you are using Wolters Kluwer, click **Regulatory Compliance > WK Regulatory Events** and then click **Wolters Kluwer Rules Engine**.
4. Select the rules that you want to enable or disable by clicking the check boxes in the first column.
The **Enabled** column displays a check mark for rules that are enabled and an **X** for rules that are disabled.
5. Click **Enable** or **Disable**.
6. Clear all check boxes to hide the toolbar.

Editing rules

You can edit rules to change their conditions, target actions, users and groups, and criticality. You cannot change the name of a rule.

About this task

To do this task, you need the **SOX > Administration > Rules Engine** permission.

Procedure

1. Log in to the Task Focused UI.
2. Click  to open the Primary menu.
3. Do one of the following steps:
 - If you are using Thomson Reuters Regulatory Intelligence, click **Regulatory Compliance > TRRI Regulatory Events** and then click **TRRI Rules Engine**.
 - If you are using Wolters Kluwer, click **Regulatory Compliance > WK Regulatory Events** and then click **Wolters Kluwer Rules Engine**.
4. Click the name of the rule that you want to edit.
Tip: To sort the rules, click a column heading.
5. Make your changes.
You cannot change the **Name** of the rule.
6. Click **Done**.

RCM Theme Deployer

The RCM Theme Deployer is a tool that you can use to automatically create requirements that are ready for assessment. The tool can also automatically create the appropriate associations.

The RCM Theme Deployer helps you to create the theme structure for business entities. Once you select a theme to deploy to the business entities, the structure is created, including the compliance plan, compliance theme, and the relevant requirement evaluation records beneath the theme, linked to the relevant Control objects.

Users can launch the Theme Deployer in two ways: from the Compliance Theme object (pushing a theme out to business entities) or from the Compliance Plan object (pulling themes into a specific business entity).

The Theme Deployer creates the Compliance Theme object and its related child requirements, represented as Requirement Evaluation (ReqEval) objects. The ReqEval objects are used to evaluate the requirements in an assessment. An association is created between the library Requirement object and the ReqEval object.

You can also link the ReqEval and relevant control instances in that area of the business.

You can also copy library instances of the related customer controls that do not already exist in the target business area.

Note: When users run the RCM Theme Deployer, they will be copying and/or linking objects from the configured Library folders to the configured business entity objects. The users must have the following security access:

- Read access to the Library folders they are copying from
- Read, Write, and Associate access to the business entity objects that they are writing to

Process overview for the RCM Theme Deployer

You can set up the IBM OpenPages Regulatory Compliance Management Theme Deployer if you have the 7.3 or later solutions schema.

If you did a fresh installation of 8.2 with solutions, the IBM OpenPages Regulatory Compliance Management Theme Deployer is already installed. Do the following steps to complete the setup:

- [“Configuring the RCM profile” on page 1067](#)
- [“Setting up auto-naming for RCM objects” on page 1067](#)
- [“Using the RCM configuration tool” on page 1068](#)

If you upgraded to 8.2, you might need to do some post-upgrade steps.

- If you used the RCM Theme Deployer in version 7.3.0.1 or later, you do not need to do any additional steps after you upgrade OpenPages.
- If you upgraded from a fresh installation of 7.3.x with solutions and you did not use the RCM Theme Deployer in your earlier version, do the following steps to set up the RCM Theme Deployer.
 - [“Installing the RCM Theme Deployer” on page 1066](#)
 - [“Configuring the RCM profile” on page 1067](#)
 - [“Setting up auto-naming for RCM objects” on page 1067](#)
 - [“Using the RCM configuration tool” on page 1068](#)

Installing the RCM Theme Deployer

If you upgraded to IBM OpenPages with Watson 8.2 or later and you want to use the IBM OpenPages Regulatory Compliance Management Theme Deployer, you need to install it.

About this task

Install the IBM OpenPages Regulatory Compliance Management Theme Deployer to make the tool available to your RCM users.

You can install the RCM Theme Deployer if your environment meets the following requirements:

- You upgraded from a fresh installation (not an upgrade) of OpenPages with Watson version 7.3.0.0 or later.
- You have the 7.3 or later solutions schema.

Note: If you did a fresh installation of version 8.2 or later with solutions, you do not need to install the RCM Theme Deployer. Skip this procedure and continue with the setup. See [“Process overview for the RCM Theme Deployer”](#) on page 1065.

Procedure

1. Log on to the admin application server as a user with administrative privileges.
2. Go to the `<OP_HOME>/installer/migration/upgrade/Module/loaderdata/RCM` directory.
3. Edit the `Environment_Variables.bat | .sh` file.

Set the following parameters for your environment at the beginning of the file. This file is used by all loading scripts.

```
openpages_domain_folder=<OP_HOME>/bin
login_username=<OP_Admin_Username>
login_password=<OP_Admin_Password>
loader_data_folder=<OP_HOME>/installer/migration/upgrade/Module/loaderdata/RCM
```

4. Go to the `<OP_HOME>/bin/` directory.
5. Edit the `ObjectManager.properties` file and set the following property to true.

```
configuration.manager.force.update.application.strings=true
```

6. Go to the `<OP_HOME>/installer/migration/upgrade/Module/loaderdata/RCM` directory.
7. Run the `Load_RCM_Config.bat | .sh` script.
8. For security purposes, remove the password from the `Environment_Variables.bat | .sh` file.
9. Edit the `<OP_HOME>/bin/ObjectManager.properties` file and set the following property to false.

```
configuration.manager.force.update.application.strings=false
```

10. Restart the OpenPages admin application server.
For more information, see [Chapter 24, “Starting and stopping servers,”](#) on page 841.
11. Configure the IBM OpenPages Regulatory Compliance Management profile.
See [“Configuring the RCM profile”](#) on page 1067.
12. Set up auto-naming for the CompliancePlan object.
See [“Setting up auto-naming for RCM objects”](#) on page 1067.
13. Configure IBM OpenPages Regulatory Compliance Management.
See [“Using the RCM configuration tool”](#) on page 1068.

Configuring the RCM profile

Use this procedure to configure the IBM OpenPages Regulatory Compliance Management profile so that you can use the RCM Theme Deployer.

Before you begin

The RCM Theme Deployer must be installed. For more information, see [“Installing the RCM Theme Deployer”](#) on page 1066.

Procedure

1. Log in to OpenPages as a user with administrative privileges.
2. Go to **Administration > Profiles**.
3. Click **OpenPages RCM Master**.
4. Update the **CompliancePlan** object.
 - a) Click the **CompliancePlan** object type.
 - b) Under **Object Fields**, click **Include** and add the field RCM-ComPlan:Theme Deployer as **Display Type URL**.
 - c) Click **Object Views**.
 - d) Click **Detail**.
 - e) Click **Choose Fields** and add the RCM-ComPlan:Theme Deployer field to the Detail view. Set the field to read-only.
5. Update the **ComplianceTheme** object.
 - a) Click the **ComplianceTheme** object type.
 - b) Click **Include** and add the field RCM-Theme:Theme Deployer as **Display Type URL**.
 - c) Click **Include** and add the field RCM-Theme:Theme Type as **Display Type List**.
 - d) Click **Detail** under **Object Views**.
 - e) Click **Choose Fields** and add the RCM-Theme:Theme Deployer field to the Detail view. Set the field to read only.
6. Enable the libraries.
 - a) Click the **CompliancePlan** object type.
 - b) Click **Detail** under **Object Views**.
 - c) Clear **Read only** on the **Library ID** field.
 - d) Click the **ComplianceTheme** object type.
 - e) Click **Detail** under **Object Views**.
 - f) Clear **Read only** on the **Library ID** field.
 - g) Click the **Requirement** object type.
 - h) Click **Detail** under **Object Views**.
 - i) Clear **Read only** on the **Library ID** field.
 - j) Click the **ReqEval** object type.
 - k) Click **Detail** under **Object Views**.
 - l) Clear **Read only** on the **Library ID** field.

Setting up auto-naming for RCM objects

You must set up auto-naming for the CompliancePlan object. Optionally, you can also set up auto-naming for the ComplianceTheme and ReqEval objects.

Procedure

1. Log in to OpenPages as a user with administrative privileges.
2. Go to **Administration > Settings**.
3. Set up auto-naming for the CompliancePlan object.
 - a) Expand the **GRCM > Auto Naming > CompliancePlan > Auto-Named** folder.
 - b) Set the value of **Copied Object** to True.
 - c) Set the value of **New Object** to True.
4. Set up auto-naming for the ComplianceTheme object.
 - a) Expand the **GRCM > Auto Naming > ComplianceTheme > Auto-Named** folder.
 - b) Set the value of **Copied Object** to True.
 - c) Set the value of **New Object** to True.
5. Set up auto-naming for the ReqEval object.
 - a) Expand the **GRCM > Auto Naming > ReqEval > Auto-Named** folder.
 - b) Set the value of **Copied Object** to True.
 - c) Set the value of **New Object** to True.

Using the RCM configuration tool

You can use the RCM configuration tool to configure IBM OpenPages Regulatory Compliance Management (RCM).

About this task

When you type fields, use the format *<Field Group>:<Field Name>*, ensure that no spaces exist before and after the colon. For example, type RCM-Req:Req Owner. For system fields, you can type just the field name.

To add another field, click the plus sign, and then type the field.

Note: Rich text fields are shown in plain text in the RCM Theme Deployer.

Procedure

1. Log in to OpenPages as an administrator.
2. Open the RCM configuration tool in a new browser tab or window.

The URL is:

```
http://<hostname>:<port>/app/solutions/rcm/config/showConfig#/editconfig
```
3. Log in with your OpenPages user account. You must be a member of the OPAdministrators group to access the tool. You can have the tool open and simultaneously be logged in to OpenPages to work on other administration tasks.
4. Expand the **Common Properties** section.
5. Enter the following information.

RCM uses these paths to locate the libraries. Use a forward slash (/) as a separator. For example, enter /Library/Control.

 - a) Enter the path for the **Control Library Folder**.
 - b) Enter the path for the **Requirement Library Folder**.
 - c) Enter the path for the **Theme Library Folder**.
 - d) Enter the path for the **Root Entity Folder**.

The **Root Entity Folder** is used to locate the business unit hierarchy.
6. Expand the **Theme Deployer Properties** section.

7. Under **Control Deployment Options**, select one or more of **Create & Link**, **Link**, and **None**.

These options define the deployment of controls during the deployment of themes. The selections that you make are displayed as options to the end user within the **Theme Deployer** helper.

- Select **Create & Link** to give the end user the option to create controls, if they do not exist, and to associate existing controls to the deployed Requirement Evaluation (ReqEval) objects.
- Select **Link** to give the end user the option to associate existing controls to the deployed Requirement Evaluation objects. New objects are not created.
- Select **None** to give the end user the option of not deploying any controls during the theme deployment process.

8. In the section **Theme Fields to be Copied**, specify the fields to be copied from the Theme Library to the deployed Compliance Theme.

By default, the field to be copied is set to **Name**, unless auto-naming is enabled. For information about auto-naming, see [“Setting up auto-naming for RCM objects” on page 1067](#).

9. In the section **Requirement Fields to be Copied**, specify the fields to be copied from the library Requirement object to the Requirement Evaluation object that is created during deployment.

By default, the field to be copied is set to **Name**, unless auto-naming is enabled.

During the copy process, a new Requirement Evaluation (ReqEval) object is created. This object might use different field groups and fields than its parent Requirement.

If the source and target fields are different, type the fields separated by the vertical line character (|). For example, type RCM-Req:Overall Req Score|RCM-Req-Eval:Applied Overall Rating.

10. If you selected the **Create & Link** option, use the **Control Fields to be Copied** to enter the fields to be copied from the library Control object to the Control object that is created during the deployment process.

By default, the field to be copied is set to **Name**, unless auto-naming is enabled.

This field applies only if you selected **Create & Link** as a control option, because this option creates a Control during the deployment process.

11. In the section **Define BE Grid Columns**, enter the Business Entity grid columns to be displayed in the helper when accessed through the Compliance Theme.
12. In the section **Define Theme Grid Columns**, enter the Theme grid columns to be displayed in the helper when accessed through the Compliance Plan.
13. Click **Validate** to validate your entries.

The folder paths are validated to ensure that they are in the correct format, and that the folders exist.

The fields are validated to ensure that the fields that you selected in **Define BE Grid Columns** and **Define Theme Grid Columns** exist in the application.

14. Click **Save**.

Chapter 38. Configuring IBM OpenPages Third Party Risk Management

You can configure IBM OpenPages Third Party Risk Management (TPRM).

For example, you can import data from SecurityScorecard and Supply Wisdom.

SecurityScorecard connector for IBM OpenPages Third Party Risk Management

IBM OpenPages Third Party Risk Management (TPRM) includes a connector for SecurityScorecard.

The SecurityScorecard connector enables you to import security ratings from SecurityScorecard into Vendor objects in OpenPages. You can then view the ratings in OpenPages.

Note: To use the connector, you must meet the following prerequisites:

- You must have a SecurityScorecard subscription. Work with SecurityScorecard to set up access. For more information, contact SecurityScorecard.
- You must install the SecurityScorecard connector. For more information, contact IBM OpenPages Support.
- In SecurityScorecard, add vendors to your portfolio. You can use your default portfolio or create a new portfolio.

When OpenPages imports ratings from SecurityScorecard, it does the following tasks:

- Looks for vendors in OpenPages that match the companies in your SecurityScorecard portfolio. based on the Vendor URL field.
- If the vendor exists in OpenPages, updates the fields in the Vendor object with the ratings from SecurityScorecard.
- If the vendor does not exist in OpenPages, creates a new Vendor object with the data from SecurityScorecard.

Importing a certificate for SecurityScorecard into the local trust store

You must import a certificate from SecurityScorecard to the local trust store. The certificate is needed to build a secure connection between the OpenPages with Watson application servers and the SecurityScorecard server.

About this task

Complete this task even if you do not use SSL/TLS.

Procedure

1. Get the certificate from SecurityScorecard and copy it to the OpenPages with Watson application server.
To get a certificate, contact SecurityScorecard.
2. Log on to the OpenPages with Watson application server.
3. Import the certificate to WebSphere Liberty by running the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_NAME> -keystore  
<STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- <CERTIFICATE_ALIAS> is the alias of the certificate that you received from SecurityScorecard.
- <CERTIFICATE_NAME> is the file name of the certificate.
- <STORE_PATH> is the full path and file name of the trust store on the application server. For example: <OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security/key.p12
- <STORE_PASSWORD> is the password of the trust store on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

4. Restart the OpenPages with Watson services.
5. Repeat these steps on each application server.

Configuring the SecurityScorecard connector

Configure the import of SecurityScorecard data into IBM OpenPages with Watson.

Before you begin

To connect to SecurityScorecard, you need all of the following items:

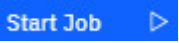
- A TLS/SSL certificate from SecurityScorecard. For more information, see [“Importing a certificate for SecurityScorecard into the local trust store”](#) on page 1071.
- Your SecurityScorecard API token.
- The name of the portfolio in SecurityScorecard that contains the data that you want to import.

About this task

To do this task, you need the following application permissions:

- **SOX > Administration > Security Scorecard Feed**
- **SOX > Administration > Scheduler**

Procedure

1. Log in to the Task Focused UI.
2. Click  > **Solution Configuration > Scheduler**.
3. Click the **Security Scorecard** job.
4. Click **Edit**.
5. Configure the connector:
 - Click **Portfolio** and type the name of your SecurityScorecard portfolio. The default is called **My Portfolio**.
 - Click **Token** and type your SecurityScorecard API token.
 - Verify the value in the **Host** field.
 - In the **Schedule** section, click **Edit**. Set the schedule for the import from SecurityScorecard.
6. Click **Done**.
The connector is configured and the import is scheduled.
7. If you want to import data from SecurityScorecard now, click the checkbox next to the **Security Scorecard** job and then click .

What to do next

To see the progress of an import, go to  > **Solution Configuration** > **Scheduler**. click the **Security Scorecard** job, and then click the **Executions** tab. Click a process to view the log.

Supply Wisdom connector for IBM OpenPages Third Party Risk Management

IBM OpenPages Third Party Risk Management (TPRM) includes a connector for Supply Wisdom.

You can use the Supply Wisdom connector to import vendor details and ratings from Supply Wisdom into Vendor objects in OpenPages. You can then view the ratings in OpenPages.

Note: To use the connector, you must meet the following prerequisites:

- You must have a Supply Wisdom subscription. Work with Supply Wisdom to set up access. For more information, contact Supply Wisdom.
- You must install the Supply Wisdom connector. For more information, contact IBM OpenPages Support.

When OpenPages imports data from Supply Wisdom, the import process does the following tasks:

- Looks for vendors in OpenPages that match the vendors in your Supply Wisdom subscription.
- If the vendor exists in OpenPages, the import process creates a Supply Wisdom object as a child of the Vendor object. The risk ratings are stored in the Supply Wisdom object. The Supply Wisdom objects are created under /BusinessEntity/Library/SupplyWisdom.
- If a Supply Wisdom object already exists for the Vendor, the import process updates the fields in the Supply Wisdom object with the risk scores from Supply Wisdom. The Supply Wisdom object stores the current scores and the scores from the previous four quarters.
- If the vendor does not exist in OpenPages, the import process creates a Vendor object and a Supply Wisdom object with the data from Supply Wisdom.

Importing a certificate for Supply Wisdom into the local trust store

You must import a certificate from Supply Wisdom to the local trust store. The certificate is needed to build a secure connection between the OpenPages with Watson application servers and the Supply Wisdom server.

About this task

Complete this task even if you do not use SSL/TLS.

Procedure

1. Get the certificate from Supply Wisdom and copy it to the OpenPages application server.
To get a certificate, contact Supply Wisdom.
2. Log on to the OpenPages application server.
3. Import the certificate to WebSphere Liberty by running the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_NAME> -keystore  
<STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- <CERTIFICATE_ALIAS> is the alias of the certificate that you received from Supply Wisdom.
- <CERTIFICATE_NAME> is the file name of the certificate.
- <STORE_PATH> is the full path and file name of the trust store on the application server. For example: <OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/key.p12

- <STORE_PASSWORD> is the password of the trust store on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

4. Restart the OpenPages with Watson services.
5. Repeat these steps on each application server.

Configuring the Supply Wisdom connector

Configure the import of Supply Wisdom data into IBM OpenPages with Watson.

Before you begin

To connect to Supply Wisdom, you need all of the following items:

- A TLS/SSL certificate from Supply Wisdom. For more information, see [“Importing a certificate for Supply Wisdom into the local trust store”](#) on page 1073.
- The Supply Wisdom URL.
- Your Supply Wisdom username and password.

About this task

To do this task, you need the following application permissions:

- **SOX > Administration > SupplyWisdom Feed**
- **SOX > Administration > Scheduler**

Procedure

1. Log in to the Task Focused UI.
2. Click  > **Solution Configuration > Scheduler**.
3. Click the **SupplyWisdom** job.
4. Click **Edit**.
5. Configure the connector:
 - Click **Password** and type your Supply Wisdom username.
 - Click **Username** and type your Supply Wisdom username.
 - Verify the value in the **Host** field.
 - In the **Schedule** section, click **Edit**. Set the schedule for the import from Supply Wisdom.
6. Click **Done**.
The connector is configured and the import is scheduled.
7. If you want to import data from Supply Wisdom now, click the checkbox next to the **SupplyWisdom** job and then click .

What to do next

To see the progress of an import, go to  > **Solution Configuration > Scheduler**, click the **SupplyWisdom** job, and then click the **Executions** tab. Click a process to view the log.

Appendix A. The Notification Manager

The Notification Manager is a JSP-based report and notification add-on utility for IBM OpenPages with Watson. It automatically creates notification emails when specified criteria are met.

Note:

- If you are using IBM OpenPages for IBM Cloud Pak for Data, use a JSP report job in the Scheduler instead. The Notification Manager is not available in IBM OpenPages for IBM Cloud Pak for Data. For more information, see [“Defining a job that runs a JSP report”](#) on page 554.
- If you are using IBM OpenPages with Watson, consider using a JSP report job in the Scheduler instead of the Notification Manager. For more information, see [“Defining a job that runs a JSP report”](#) on page 554.

With the Notification Manager, administrators can define a set of object properties and values that trigger the sending of a notification email to a user. The user responsible for the item will receive the email, alerting the user to their necessary tasks.

For example, a notification event can be set to run nightly that will send a notification email to all users who have Tests that do not have completed Test Results associated with them.

To use the Notification Manager tool, you need the **SOX > Administration > Notification Manager** application permission.

Why would I use Notifications?

Notifications allow you to alert people that important dates are approaching, and remind them that they still have outstanding tasks to perform before the date arrives.

Since notification can be tied to the value of an object property, you can target the reminder to only those people who meet the criteria for the notification.

For example, you can set up a notification to remind all Control owners who have controls that have a value of "Undetermined" for the Control Evaluation field, and set the notification to start 20 days after the beginning of the quarter.

The notification reports

The report pages and page templates that are required to set up a notification event must be in the Reporting/[locale]/SOX/Notifications folder.

Use the **Manage Pages and Templates** task in the Task Focused UI to access the Reporting/[locale]/SOX/Notifications folder.

Results of running a notification report

When a notification report is run, a notification e-mail is generated for the Executive or Primary Owners detailing the objects that require attention.

Requirements for setting up a notification

In order to set up a notification event, you must have the following:

- A user account with the **Publishing** application permission set. For more information, see [“Application permissions not contained under the SOX heading”](#) on page 97)
- Administrator access to the IBM OpenPages with Watson server machine (for scheduling reports to run automatically)

Tip: You can also run Notification Manager from a remote system, such as your laptop. For more information, see [“Installing tools and utilities \(IBM OpenPages with Watson\)” on page 824](#)

- Your notification mail server configured. For more information, see [“Set the mail server address” on page 612](#).

Setting up a notification

Three procedures are required to set up and execute a notification.

- [“Task 1: Creating a page template ” on page 1076](#)
- [“Task 2: Creating the notification” on page 1076](#)
- [“Task 3: Triggering the notification” on page 1077](#)

After each task is completed, you can run the notification manually or schedule it to run automatically.

Task 1: Creating a page template

The first step in setting up a notification is to create a page template that the notification report is based on.

Before you begin

Ensure that your objects have the necessary information that will be required by the notification report. If the objects are not up-to-date, the report will not find the data it needs and will either return a sub-set of the entire results, or fail to run at all.

Procedure

1. Log on to the OpenPages with Watson Task Focused UI as a user with **Publishing** privileges set.
2. Click  > **System Configuration** > **Pages and Templates**.
3. Navigate to the SOX/[locale]/Notifications folder and select it with a check mark.
4. Click **Add Page Template**. The **New Page Template** screen is displayed.
5. Do the following:
 - a) Enter a name for the page template.
 - b) Select an **Output file extension**.
 - c) Select a **Template JSP**.
 - d) Click **Save** to continue.
 - e) Enter a description for the page template.
 - f) Click **Save** to save your changes.

Task 2: Creating the notification

The second task in setting up a notification is to create the notification.

Procedure

1. Log on to the OpenPages with Watson Task Focused UI as a user with **Publishing** privileges set.
2. Click  > **System Configuration** > **Pages and Templates**.
3. Navigate to the SOX/[locale]/Notifications folder and select it with a check mark.
4. Click **Add Page**. The **Add a Page** screen is displayed.
5. Do the following:
 - a) Enter a name and description for the notification report.
 - b) Choose the page template that you already created in Task 1.

- c) Click **Save** to continue.
- d) Enter the information for your notification type in **Page Details**.
- e) Click **Save** to save your changes.

Task 3: Triggering the notification

You can run notification reports from the Reporting interface like any other report, or you can use the provided command line interface to run the notification reports from outside the IBM OpenPages with Watson environment.

Tip: You can also run Notification Manager from a remote system, such as your laptop. For more information, see [“Installing tools and utilities \(IBM OpenPages with Watson\)”](#) on page 824

If you are using IBM OpenPages for IBM Cloud Pak for Data, use a JSP report job in the Scheduler instead. The reporting interface and the Notification Manager utility are not available in IBM OpenPages for IBM Cloud Pak for Data. For more information, see [“Defining a job that runs a JSP report”](#) on page 554.

Using the application user interface

Running a notification report from the IBM OpenPages with Watson user interface works the same as running any other report through the user interface.

Note: You cannot use the Preview function in the OpenPages with Watson Standard UI with Notification reports.

Procedure

1. Log on to the OpenPages with Watson Standard UI and click the **Reporting** menu on the menu bar.
2. Click the **Notifications** sub-menu to display the notification reports.
3. Choose the notification report you want to run and click the name of the report.

The results of the report are displayed in a new browser window.

Using the Notification Manager command line interface

You can manually run the Notification Manager from a command or shell window, or you can use standard operating system scheduler functions to automatically run the Notification Manager command file at a specified time.

For example, in Windows, you could use the built-in Windows scheduler. In Linux, you could set up a cron job.

You can run a single report, an entire folder of reports, and run a single report against multiple datasets by providing parameters to the report directly through the command line.

The Notification Manager command file is named as follows:

Windows

NotificationManager.cmd

Linux

NotificationManager.sh

The file is located in the `<OP_Home>|bin` directory of your IBM OpenPages with Watson installation.

The Notification Manager command line interface syntax

This topic contains the Notification Manager command line interface syntax and parameters.

Syntax

```
NotificationManager -Username <user_name> -Password <password>  
-NotificationProgram <full_path_to_notification_report>|-ProgramFolder  
<path_to_folder-containing-notification-reports> [-SaveOutput <true|false>]  
[-LogSession <true|false>]  
[-<parameter_name> <parameter_value>] [-ParameterFile <full_path_to_file>]
```

Parameters

All parameters are in the syntax -parameter "value or string". If the value of any parameter contains spaces, that value must be contained within quotation marks.

Table 308. Notification Manager parameters	
Parameter	Description
-Username	The name of a valid IBM OpenPages with Watson user with permission to run the notification reports.
-Password	The password for the user name set in -Username.
-NotificationProgram	(Required unless -ProgramFolder is specified) The full path to the notification report the command will run, starting with the Reporting folder. Should not begin with a leading slash. Example <pre>-NotificationProgram "Reporting\SOX\Notifications\ Test Notifications Report"</pre>
-ProgramFolder	(Required unless -NotificationProgram is specified) Specifies a folder containing notification reports. All reports in that folder will be executed when the command is run. Example <pre>-ProgramFolder "Reporting\SOX\Notifications"</pre>
-SaveOutput	(Optional) Can be true or false. If set to true, the output of the report will be saved to an output file in the output_files directory under the bin NotificationManager directory. If the parameter is not present, no output file will be created. The file name is the name of the notification report (or folder) with an "html" extension. If an output file with that name already exists, a timestamp extension will be added to the end of the existing file's name and the older file will be moved to the output_files archive folder. Example <pre>Undetermined Controls.html.200406060103</pre>
-LogSession	(Optional) Can be set to true. If set, the activities of the NotificationManager will be written to a log file. The log file will be located in the logs directory under the aurora bin NotificationManager directory. The name of the log file is NotificationManager.log. The file has a maximum size of 1 MB, and will be rotated into the logs archives directory when the limit is exceeded.

Table 308. Notification Manager parameters (continued)

Parameter	Description
-<parameter_name> <parameter_value> Where: <parameter_name> is the name of a specific parameter <parameter_value> is the value of that parameter	(Optional) If you want to pass a value for a specific notification report parameter, you can include the parameter and value directly in the command line. The parameter name must match the report parameter name exactly. The parameter names can be viewed by logging on to the OpenPages with Watson Task Focused UI. Use the Manage Pages and Templates task to navigate to the folder that contains the report page. The parameter names are shown in the detail page for the report page. Examples • -mailServer mail.openpages.com • -generalMessage "Please do not ignore this e-mail."
-ParameterFile	Specifies a text file containing a list of parameter value pairs (equivalent to entering individual -parameter "value or string" entries into the command line directly). Each parameter value pair should be on a single line. Value is the full path to the file, including the file name. Example - for Windows: <pre>-ParameterFile "c:\OpenPages\bin\NotificationManager\notification_parameters.txt"</pre>

Appendix B. Properties and parameters

IBM OpenPages with Watson includes different properties files. Depending on the configuration task that you perform, you edit one or more of the properties files.

Aurora properties and parameters

Depending on the configuration task that you perform in IBM OpenPages with Watson, you might need to edit the parameters in the `aurora.properties` file.

The `<OP_HOME>/aurora/conf/aurora.properties` file parameters are described in the following list.

Note: If you change the parameter values, you must restart the application servers.

Application server properties

aurora.appserver

The type of Java Platform Enterprise Edition (J2EE) application that is used.

Possible value: `websphere`.

aurora.initialcontext.factory

Java Naming and Directory Interface (JNDI) initial context factory.

Database properties

database.type

Type of database (Oracle or DB2).

database.URL

Java Database Connectivity (JDBC) URL.

database.DRIVER

Java Database Connectivity (JDBC) driver.

database.USERID

Database user name.

database.PASSWORD

Database password (encrypted).

IBM Db2 database properties

database.NAME

Database name.

database.HOSTNAME

Database host name.

database.PORT

Database port.

database.CATALOG_NAME

Database catalog name.

Database pool properties

database.pool.minsize

Minimum number of connections.

database.pool.maxsize

Maximum number of connections.

database.pool.refresh.interval

Database pool refresh interval.

database.pool.testonreserve

Flag to test a connection before returning it from the pool.

Possible values: true or false.

Database connection test property**database.test.connection.sql**

Specify a Microsoft SQL database with which to test the connection.

The default value is: *select sysdate from dual.*

Java Transaction API (JTA) properties**jta.initialcontext.factory**

Java Naming and Directory Interface (JNDI) Initial Context Factory.

jta.jndi.transaction

Java Naming and Directory Interface (JNDI) name for User Transactions.

Full text search properties**fulltext.index.directory**

Full text index folder.

fulltext.index.exclude

File extensions to be excluded.

The default values are: xra xrl pagespec pagetemplate xrt cha xsd.

Java Message Service (JMS) properties**jms.initialcontext.factory**

Java Naming and Directory Interface (JNDI) Initial Context Factory.

jms.topic.RepositoryTopic

Java Message Service (JMS) topic name.

jms.topic.ResourceCacheTopic

Java Message Service (JMS) topic name.

Security service properties**security.accesstoken.timeout**

Session token timeout, in minutes.

The default value is 3000000.

security.system.password

Password of the system OPSysSystem user.

AppServer specific properties**appserver.install.directory**

The installation folder of OpenPages application.

Third-party reporting-specific properties**cognos.server**

Server URL of Cognos.

cognos.framework.refresh.servlet

Framework refresh URL.

cognos.report.output.dir

Temporary folder for reports.

cognos.computation.server

Cognos computation server URL.

Logout URL property

Add new URLs with the name `logout.url.<name>`. The name can be anything.

logout.url.cognos

Cognos logout URL.

Application URL property**application.url.path**

Base URL of the application.

Application server WorkManager properties**workmanager.jndi.name**

Java Naming and Directory Interface (JNDI) name of the application server work manager.

workmanager.impl.classname

Work manager implementation class.

Enterprise JavaBeans (EJB) properties**server.use.local.ejb**

Must be `true` in 8.2.x and later.

Other properties**enforce.browser.support**

Enables or disables the **Allowed Browsers** feature. For more information, see [“Specify the browsers that can access IBM OpenPages” on page 603](#).

Value: `true` or `false`

OpenPages server properties and parameters

Depending on the configuration task that you perform in IBM OpenPages with Watson, you might need to edit the parameters in the `Server<#>-server.properties` file.

The OpenPages server properties are described in the following list.

Note: If you change the property values, you must restart the application servers.

Cache properties**cache.synchronizer.classname**

Non-configurable system parameter.

cache.listener.enabled

Non-configurable system parameter.

cache.notifier.enabled

Non-configurable system parameter.

jms.topic.CacheTopic

Non-configurable system parameter.

URL properties

url.path.openpages

Configurable application URL.

Value: `http\://<hostname>\:<port>/openpages`

Where

- *hostname* is fully qualified, and includes the local host and the parent domain name.
- *<port>* is the OpenPages application port number (default for non-SSL: 10108). For more information, see [“Updating the application port values in the server and tools client properties files” on page 766.](#)

Web client properties

webclient.http.server.protocol

Enter the value `http` or `https`, based on your configuration. The default value is `http`.

webclient.http.server.name

Non-configurable system parameter.

webclient.http.server.port

If you change the OpenPages application port number (default for non-SSL: 10108), update the application port value in this parameter.

Other

async.calculation.enabled

Enables or disables asynchronous processing of calculations.

If you are using clustered application servers, setting this property to `true` can help performance by managing the processing workload for calculations. You can enable or disable this property on a server-by-server basis to control the workload.

Value: `true` or `false`

Sosa properties and parameters

Depending on the configuration task that you perform in IBM OpenPages with Watson, you might need to edit the parameters in the `Server<#>-sosa.properties` file.

The `Server<#>-sosa.properties` file parameters are described in the following list.

Note: If you change the parameter values, you must restart the application servers.

Application URL properties

application.url.path

Configurable application URL.

`http\://<hostname>\:<port>/openpages`

Where:

- *hostname* is fully qualified, and includes the local host and the parent domain name.
- *<port>* is the OpenPages application port number (for example, 10111).

application.context

Configurable application context.

`/openpages`

Service URL properties

openpages.service.initial.ctx.factory

Non-configurable system parameter.

Tools properties and parameters

Depending on the configuration tasks that you perform in IBM OpenPages with Watson, you might need to edit the properties in the `openpages-tools-client.properties` file.

The `openpages-tools-client.properties` file is used by OpenPages tools such as ObjectManager Notification Manager, and command-line utilities.

The file is located on each application server in the `<OP_HOME>/bin` directory.

rest.url.path

The base URL of the public REST API on the application server.

IBM OpenPages with Watson

```
https\://<host>\:<port>/grc/api
```

Replace `<host>` with `localhost` or with the hostname of the OpenPages application server. You can use `localhost` if the tools and utilities will be run on the application server.

Replace `<port>` with the OpenPages application server's port number.

For example:

```
https\://localhost\:10111/grc/api
```

IBM OpenPages for IBM Cloud Pak for Data

```
https\://<cpd_url>/openpages-<instance_name>-grc
```

Replace `<cpd_url>` with the URL of IBM Cloud Pak for Data. Replace `<instance_name>` with the name of the OpenPages instance.

insecure.skip.tls.verify

If set to `true`, the application server's TLS (SSL) certificate is not checked for validity when you run tools such as ObjectManager.

If set to `false` or if the `insecure.skip.tls.verify` is not specified in the `openpages-tools-client.properties`, the application server's certificate is checked for validity. The TLS check occurs when a tool (such as ObjectManager) communicates with the REST API on the application server. The check passes if either of the following conditions is true:

- The server's certificate is valid (it is not self-signed).
- The server's certificate is self-signed but exists in the client's truststore.

Allowed values: `true` or `false`

Default value: `false`

If the URL in `rest.url.path` uses HTTP, the `insecure.skip.tls.verify` property is ignored.

max.req.body.size.mb

The maximum request size (in MB) of requests that are sent from client tools, such as ObjectManager, to the server's REST API. A request that is larger than this threshold is automatically divided into chunks, which are then sent separately.

For example, suppose that your web server sets an upload limit of 50 MB. This upload limit means that any requests from client tools must be smaller than 50 MB. To meet this requirement, you can set `max.req.body.size.mb=50`. Now, suppose that you use ObjectManager to load 100 MB of data. Your upload is automatically broken down into two 50 MB chunks so that the upload does not exceed the 50 MB threshold.

Appendix C. Non-role based access control

You can use non-role based access control for backward compatibility with IBM OpenPages Governance Platform 5.1x (and earlier).

The custom security feature is deprecated. For flexible role-based security administration, it is best to migrate your access control data to the role-based security model. For details, see [“Role-based security model” on page 105](#)). For assistance with upgrading your system, contact IBM OpenPages Support.

Using non-role based security, administrators can grant or deny read, write, delete, and associate permissions to groups or specific users based on folders. These permissions are set using an Access Control List, or ACL. An ACL is the list of groups and users who have permissions for the specified folder. You can explicitly set permissions on folders or inherit permissions from a parent folder.

You can set up security for non-role based access control, which can be set to control the ability to read, write, delete, and associate the objects in a folder. Each of these settings can be set individually, allowing fine-level control over user and group access to the contents of a folder. Any folders that contain IBM OpenPages Governance Platform 5.1x (and earlier) objects (business entities, accounts, risks, etc.) can be administered through ACLs.

The **Custom Security** task is available in both the Task Focused UI and the Standard UI. Changes made in one user interface are immediately reflected in the other. The procedures in this appendix explain how to complete the steps using the Standard UI.

Note: Non-role based security access control can only be set at the folder level. Individual objects within a folder cannot have ACLs - they automatically assume the ACL of the folder. If you have permissions for one item in a folder, you have the same permissions for the other objects in that folder.

Using ACLs with top-level folders

When setting up your business entity and other object hierarchy, certain folders are already created for you by the IBM OpenPages with Watson installation.

These folders are created with pre-set ACLs, and should not be modified.

Make sure you do not modify the ACLs for the following folders:

```
Default
  BusinessEntity
  ICDocumentation
  Issue
  IssueActionItems
  Plan
Files and Forms
```

The object folder structure

When the object hierarchy is viewed from the application interface, the folder structure is listed in alphabetical order, unlike the overview screens, which display relationships.

Business entities are contained in their own folder, while all of the other object types have their own folder underneath the Documentation folder.

Note: ACLs should never be added to folders that were automatically created during installation (e.g., ICDocumentation, BusinessEntity, etc.). Always create ACLs using the IBM OpenPages with Watson administrative user interface.

When you add a new business entity called Enterprise, a folder with the name of the business entity is created underneath the *BusinessEntity* folder.

When you add a sub-entity named "Region" to the "Enterprise" entity, a corresponding folder is created.

When you add other objects to a business entity hierarchy, the folder structure of the business entities it belongs to is automatically created under the object type folder. All objects of that type created for that business entity are placed in the same folder.

Important: When you are setting ACLs, it is important to remember to set ACLs for the business entity folders under the *ICDocumentation* folder structure, as well as the *Business Entity* folder structure. If you do not, when you try to access the objects you will not be able to browse to the objects. You should never set ACLs on the container folders (e.g., *ICDocumentation*, *BusinessEntity*).

Using inheritance with Access Control Lists

By default, in a non-role based access control environment, the object folder hierarchy inherits security ACLs from the higher-level folders.

If a folder does not have an ACL set for a particular group, the application looks back up the folder tree until it finds an ACL for that group and uses it for the current folder. By default, all users can edit any object in the entire project.

This setup is useful for smaller projects, where there is a single or very few teams working on the same business entity structure. In the case where you have specific users who are denied viewing or editing permissions, you can easily deny them access to a folder structure by setting an explicit ACL for the group or user that denies them access.

However, this paradigm rapidly becomes unwieldy for large numbers of groups or business entities. If you only want a group to see one region or site out of 50, it is much simpler to grant access to the single site than to deny access to the other 49.

Breaking inheritance

Using the IBM OpenPages with Watson application user interface, you can break the inheritance property on any folder.

When you break inheritance, access is limited to **ONLY** the groups and users who have an ACL for that business entity. All other groups and users (besides the creator of the object) are automatically set to Denied/Denied/Denied/Denied.

For large teams and projects who wish to restrict which areas of the project can be seen or modified, breaking the inheritance "chain" is very helpful, since it automatically denies all groups and users access to the particular business entity structure. Only the groups and users specifically included in an ACL have access to the business entity children.

Instead of denying a group access to 49 sites, as in the previous example, now you only have to grant access to the desired site, and the other 49 are denied by default.

Note: Breaking inheritance is not without its drawbacks. Because all groups (except OpenPagesAdministrators and OPAdministrators) are denied access to the business entity, groups that do not have an ACL entry cannot see the business entity or any object underneath the business entity. This is true even if an ACL entry for a specific group is added to a sub-entity. Because the group (or user) is denied Read access at the parent business entity, they cannot browse the tree to view the sub-entity where they have access. The following sections will explain how to circumvent this restriction using nested groups.

Procedure

1. Log on to the OpenPages with Watson application as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration > Custom Security**.
3. Navigate to the business entity folder where you want to break inheritance (under the *Default* directory).
4. When you have found the desired folder, click the name of the folder to display the detail page.
5. Click **Add** and choose the desired group or user from the list.

6. Choose the desired permissions for the group or user by highlighting the appropriate entries and click the **OK** icon to add the new ACL to the folder.
7. Now that a valid ACL exists for the folder, click the **Disable Inheritance** icon under the Folder heading. The value of the "Inherit ACL" field is changed to "false" and the **Disable Inheritance** icon changes to **Enable Inheritance**.
8. Click **Access Controls** in the breadcrumb trail to return to the Access Controls folder list.

Results

After you break the inheritance on a folder, the new permissions (or lack thereof) go into effect immediately. Only members of the OpenPagesAdministrators and OPAdministrators groups will be able to access the object, unless a specific ACL for a user or group is created.

Remember, no one except the groups (and sub-groups of those groups) listed in the Access Controls table will be able to see the folder or its contents.

Note:

- The OpenPagesAdministrators group and the creator of a folder or object is exempt from ACL restrictions. The creator always has Delete access to files and folders he or she has created, while the OpenPagesAdministrators group has total access to all files and folders.
- If you have broken inheritance for a folder, there will be entries for the OpenPagesAdministrators and OPAdministrators groups. These ACLs cannot be edited or deleted.

Creating an ACL on a folder

You must have the Access Control Lists application permission to view or edit ACL settings.

Procedure

1. Log on to the IBM OpenPages with Watson application as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration > Custom Security**.
3. Navigate to the folder in which you want to create a new ACL. Click the folder name to display the detail page of the folder.
4. Click **Add** to add a new access control to the list.
5. In the Create an Access Control Setting page, choose the desired group or user from the drop-down list.
6. Select the desired permissions by highlighting the appropriate choices and clicking **OK** when finished. The dialog closes, and the new ACL appears in the list area of the folder detail page.

Read permission is required for Write and Associate access, and Write access is required in order for Delete access to be granted. You can select any combination of permissions, but when you save the ACL, it will be modified to be a valid combination of permissions.

For example, if you set Read/Write/Delete/Associate to Denied/Granted/Granted/Granted, when you click **OK**, the displayed permissions will be Granted/Granted/Granted/Granted. Because users must have Read permissions in order to have Delete permissions, the Read permission is changed to "Granted".

In order to set Read to Denied, Write, Delete, and Associate must also be set to Denied.

7. Once you have finished setting the permissions, click the **Access Control** link in the Action menu to return to the Access Control list.

Editing an existing ACL

You can edit an existing ACL.

Procedure

1. Log on to the IBM OpenPages with Watson application as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration > Custom Security**.
3. Click the folder name to display the detail page with the list of existing ACLs.
4. Click the check box next to the existing ACL you wish to modify and click the **Edit** icon to display the Edit an Access Control Setting page.
5. Select the desired permissions by highlighting the appropriate choices and clicking **Save** when finished. The dialog closes, and the updated ACL appears in the list area of the Access Control page.

Read permission is required for Write and Associate access, and Write access is required in order for Delete access to be granted. You can select any combination of permissions, but when you save the ACL, it will be modified to be a valid combination of permissions.

For example, if you set Read/Write/Delete/Associate to Denied/Granted/Granted/Granted, when you click **Ok**, the displayed permissions will be Granted/Granted/Granted/Granted. Because users must have Read permissions in order to have Delete permissions, the Read permission is changed to "Granted".

In order to set Read to Denied, Write, Delete, and Associate must also be set to Denied.

For example, if you set a folder ACL for a group to Granted for Read, and leave Write and Delete blank, they will be shown in the UI as Granted/Inherited/Inherited. However, if you set the permissions to Granted for Delete, and left Read and Write blank, the ACL is displayed as Granted/Granted/Granted, since Delete requires Read and Write permissions.

Deleting an existing ACL

You can delete an existing ACL.

Procedure

1. Log on to the IBM OpenPages with Watson application as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration > Custom Security**.
3. Navigate the folder tree to display the folder containing the ACL you want to delete.
4. Click the folder name to display the detail page with the list of existing ACLs.
5. Click the check box next to the existing ACL you wish to remove and click the **Delete** icon to remove the ACL.

Using groups to establish user roles

User groups fulfill three functions - to segregate users into meaningful subsets, to define ACLs to limit both the range of actions that can be performed on a folder's contents, and to limit the scope of a user's activity to a specific folder or set of folders.

Understand how groups are used to separate a set of users into different roles within an organization.

The core IBM OpenPages Governance Platform 5.1x (and earlier) groups

The IBM OpenPages Governance Platform 5.1x (and earlier) application has two predefined user groups already created as part of the initial installation.

These groups are:

- **OpenPagesApplicationUsers** - This group is a container for all users who are part of the IBM OpenPages Governance Platform 5.1x (and earlier) application. Every IBM OpenPages

Governance Platform 5.1x (and earlier) user will be a part of this group through inheritance. The OpenPagesApplicationUsers group has a single sub-group - OpenPagesAdministrators.

Note: The OpenPagesApplicationUsers group should never be used to set ACLs on any folder. The group exists for administrative purposes only.

- **OpenPagesAdministrators** - In order to have administrative-level permissions, users must be part of this group. Administrators can customize reports, create users and groups through the IBM OpenPages Governance Platform 5.1x (and earlier) user interface, and assign and modify ACLs. They also have access to all folders and objects in the IBM OpenPages Governance Platform 5.1x (and earlier) hierarchy, regardless of ACLs.

Example: Using groups to establish user roles

Widgets, Inc. has decided that they will divide their IBM OpenPages Governance Platform 5.1x (and earlier) users into four main teams, each responsible for a different area of their financial controls documentation project.

These four teams are:

- The Executive Team. These are people who do not document or modify individual objects. As a team, they are only interested in viewing the entire financial controls documentation process as a whole, and quantifying the results. CFOs and high-level corporate users fall into this category. They need read access to almost all folders in order to run reports on the documentation project as a whole.
- The System Team. This group is responsible for setting up and maintaining the entire hierarchy of IBM OpenPages Governance Platform 5.1x (and earlier) objects. They are also the only ones allowed to modify anything above the control level. In most companies, the IT department or a sub-set of the central accounting team is responsible for these activities.
- The Regional Teams. These groups are responsible for developing, maintaining, and overseeing the objects for all of the sites within their regions.
- **The Site Teams.** These groups are responsible for documenting the controls for their sites, as well as uploading test results and control documents.

The Executive and System teams are both based in the Corporate Center, while the Regional Teams and Site Teams are located in their respective regional and site headquarters.

Although you can have user groups that correspond to the entire team, they are not necessary when setting ACLs. However, so-called "team" groups can be helpful for organizational purposes as well as assigning tasks or other uses. The important groups within each team will divide the teams according to the level of interaction (Reading, Writing, Deleting, Associating) they will be allowed, as well as the scope of the folders they can act on. These groups will be explained in the following sections.

Using groups to limit user activities

Groups are used in folder ACLs to limit what each group of users can do to the objects located in the folder.

In general, you will want a group of users who are limited to just viewing the objects, a group who can both view and edit the objects, and another group who can view, edit, associate and delete the objects.

In the following sections, we will divide each team into subgroups with different access permissions.

The executive team

The Executive team is interested mainly in the overall status of the financial controls documentation project, and gathers most of their information by running reports on the various objects and drilling down into the objects via the report links.

Some possible sub-groups of the Enterprise team are:

- FinancialOfficers

- ExternalAuditors
- InternalAuditors

In the case of the Executive Team, the sub-groups are merely organizational in nature. However, by making them sub-groups of the Executive Team group, you gain the flexibility of categorizing the Executive users by roles without adding complexity to your ACL definitions.

All of the sub-groups require the same access to the object hierarchy - they only need Read access in order to run reports and view individual objects from those reports. As an organizational grouping, the ExecutiveTeam group will not appear in any ACLs directly - rather, it will be added as a member of many other groups with read-only access.

After you create your Executive Team sub-groups, add the appropriate users to each sub-group. Users should NOT be added directly to the ExecutiveTeam group - add them to a sub-group instead.

The regional teams

Each Regional team (one for each region) is responsible for reviewing and maintaining the objects that are specific to the sites in their region.

In function, they are quite similar to the System team, but their influence is limited to all of the sites in their region.

The various sub-groups for the Regional teams are actually two levels - first you need an "umbrella" RegionalTeams group. Under that group, you need to create sub-groups for each region.

For example:

- Region01Reviewers - responsible for reviewing and reporting on all of the sites in Region 01. They require Read access to everything in Region 01.
- Region01Writers - responsible for making any necessary changes to the objects in any of the sites in Region 01. They require Read, Write, and Associate access to everything in Region 01.
- Region01Directors - responsible for deleting obsolete objects or defunct sites in Region 01. They require Read, Write, Associate, and Delete access to everything in Region 01.

You would create a set of groups for each region in your company (Region02Reviewers, Region02Writers, etc.). After you create a set of groups for each region and added all of the users from the Regional Teams who belong directly to each group, it is time to create the groups for each Site.

The site teams

Below the Regional level, each Site has its own team of Reviewers, Writers, and Directors.

For each site in each region, you would create a set of sub-groups as follows:

- R01Site01Reviewers - responsible for reviewing and reporting on Site 01 in Region 01. They require Read access to everything in Site 01.
- R01Site01Writers - responsible for making any necessary changes to the objects in Site 01 in Region 01. They require Read, Write, and Associate access to everything in Site 01.
- R01Site01Directors - responsible for deleting obsolete objects or defunct sites in Site 01 in Region 01. They require Read, Write, Associate, and Delete access to everything in Site 01.

Just like at the Regional level, you would create a set of sub-groups for each site in each Region. Although by this time we are probably creating a lot of groups, each group will only have to be declared in an ACL once at the site level.

As you create the Site groups, you can add the users who belong directly to each group. Adding groups to other groups will be handled in the next section.

Using nested groups to limit user scope

Three procedures are required to configure nested groups and limit user scope. Tasks are : break the inheritance of business entities to restrict the scope of users and groups, nest groups inside one another, and add ACLs to regions and sites.

- [“Limiting user access by breaking folder inheritance” on page 1093](#)
- [“Limiting user access by nesting user groups” on page 1093](#)
- [“Limiting user access by setting folder Access Control Lists” on page 1094](#)

Limiting user access by breaking folder inheritance

The first step in limiting user access to regions and sites is to break the inheritance of all of our business entity folders - all regions and all sites.

Breaking the inheritance sets all of the groups and users without an ACL (except those with the Access Control Lists application permission) on the business entity folder to Denied/Denied/Denied/Denied. They can't view, edit, or delete the folder, create or remove associations, or view any business entity folder underneath it, even if they have an ACL set on a lower-level folder.

Read permission is the most important. Read allows you to see folders underneath the business entity and navigate down to them. However, with many Regions and Sites to set up, we don't want to have to keep Denying access to all sorts of groups.

Procedure

1. Log on to IBM OpenPages with Watson as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration > Custom Security**.
3. Navigate to the business entity folder where you wish to break inheritance (under the *Default* directory).
4. When you have found the folder, click the name of the folder to display the detail page.
5. Click **Add** in the Access Controls table and choose the desired group or user.
6. Highlight the desired permissions for the group or user and click **OK** to add the ACL to the folder.
7. Now that a valid ACL exists for the folder, click the **Disable Inheritance** icon under the Folder heading. The value of the "Inherit ACL" field is changed to "false" and the **Disable Inheritance** icon changes to **Enable Inheritance**.
8. Click **Access Controls** in the breadcrumb trail to return to the Access Controls folder list.
9. Repeat this procedure for each business entity folder.

Note: Do not forget to modify the business entity folders under each object type in the ICDocumentation tree.

Limiting user access by nesting user groups

Now you have a lot of groups with users assigned to them according to their role.

Now, add groups to other groups in order to properly restrict their area of effect.

The way groups with users nest seems backwards at first glance - the most general groups (the System and Executive groups) have to be added to the more limited ones (the Regional groups), while the Regional groups have to be added to the most limited ones (the Site groups).

If the Region01Writers group belonged to the SystemWriters group, which can read, write, and associate to all regions, they would also be able to read and write to all Regions, which is not the desired behavior. We are trying to limit user scope, not enhance it. So adding smaller groups to larger groups doesn't work out correctly.

If you add the larger Regional groups to the smaller Site groups beneath them, you don't increase the smaller group's scope beyond its boundaries, but the Regional groups extend their vision downwards into all of the sites in their own Region. (Remember, since we broke inheritance at each level of the business entity, Regional groups don't automatically get to see the Sites underneath their Region.)

Here's a diagram that shows the way this works:

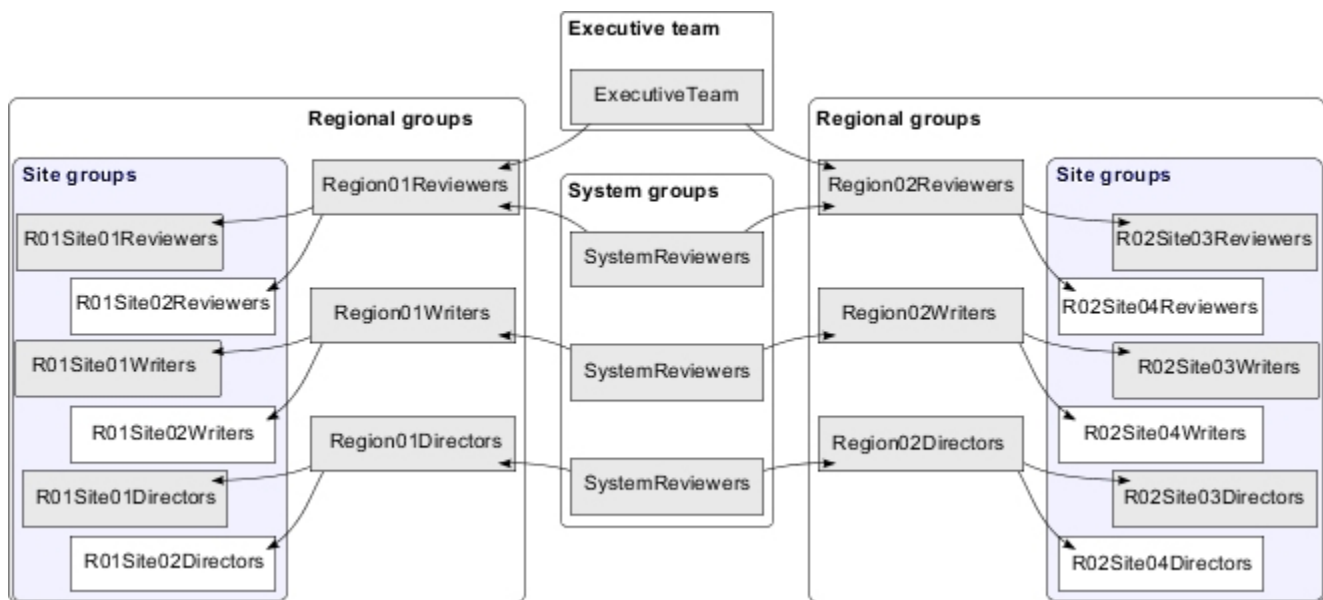


Figure 91. Nesting user groups

Let's follow one use case shown in the preceding diagram. The SystemWriters group becomes a sub-group to the Region01Writers group (and the Region02Writers group, and so on). Then, the Region01Writers group becomes a sub-group of the R01Site01Writers group (and the R01Site02Writers group, etc.). The sub-groups of Region01Writers also become sub-groups of R01Site01Writers through group inheritance. The effective members list of R01Site01Writers is now:

```
R01Site01Writers
  <writer1>
  <writer2>
  ...
  Region01Writers
    (SystemWriters)
```

In the previous example, SystemWriters is in parentheses, because it isn't explicitly added to the group - it's included as a sub-group of the RegionalXXWriters groups. The same goes for the ExecutiveTeam group; it is added to each of the RegionXXReviewers groups. Executives only need Read access, so we don't need to add them to any other ACL classification.

Note: If you are using the Library paradigm, you do not want to add the ExecutiveTeam group to the Library group. You don't want empty Library data included into the executive level reports.

Now identify how to use the nested groups to set ACLs.

Limiting user access by setting folder Access Control Lists

User groups with different permission needs are defined for each site. The next task is to create ACLs.

For each site, create an ACL for each R##Site## group and give them the necessary permissions. For example, in R01Site01, the ACLs for the business entity folder would look like this:

□	R01Site01	OPAdministrators	Granted	Granted	Granted	Granted
		SOXAdministrators	Granted	Granted	Granted	Granted
		R01Site01Reviewers	Granted	Denied	Denied	Denied
		R01Site01Writers	Granted	Granted	Denied	Granted
		R01Site01Directors	Granted	Granted	Granted	Granted

Figure 92. ACLs for the Business Entity folder

It is not necessary to specify the Region01Reviewers, Writers, or Directors. They are included as members of the R01Site01 groups!

Specify ACLs for different access control levels (Read, Write, Delete, Associate) for business entity folders that contain non-business entity objects. For example, in our hierarchy, Regions only contain the sub-entity Sites - there are no accounts, processes, etc. directly associated with a Region. Therefore, we don't have to create ACLs for Region01Reviewers and the other ACL-specific groups at the Region level. In our current example, here's the ACL list for Region01:

+ □	Region01	OPAdministrators	Granted	Granted	Granted	Granted
		SOXAdministrators	Granted	Granted	Granted	Granted

Figure 93. ACLs for the Region01

The following guidelines identify whether to create an ACL for a user group on a business entity:

- If the business entity has accounts or processes associated with it, create an ACL for each entity-specific group (such as R01Site01Writers, etc.) with the correct permissions.
- When you create ACLs for a business entity, replicate the ACL for each business entity folder underneath the ICDocumentation folder structure. For example, you must create the same ACL list for the ICDocumentation/Accounts/Region01/R01Site01 folder that you created for the BusinessEntities/Region01/R01Site01 folder, and so on through each sub-folder structure under ICDocumentation (Accounts, Processes, Risks, Controls, etc.).

Note: If no folder with the correct name exists, either no object of that type currently exists in the business entity hierarchy, or parent folder ACLs do not include a group that contains the current user, preventing you from seeing the folder.

- If a business entity only has sub-entities associated with it, you should not create individual ACLs for the business entity's Reviewer, Writer, and Director groups. We will deal with this in the next section,

Only one step remains - we've created the ACLs for our business entities, but when you log in, you can only see the first level of your business entities. We now need to establish read permissions in the business entities above our Site user groups, so that we can browse to the Site level and view our objects.

Using group ACLs to traverse business entities

Even though we have successfully created a nested series of groups that successfully limits the scope of our site users, we seem to have gone a little too far - we can't browse through the business entities to get to our site!

We need to create a group that will allow site users to browse through the entities, without granting anything but Read.

To allow Read access to lower-level user groups, complete the following steps:

Procedure

1. Access the Users, Groups and Domains page (see [Chapter 4, "Users, groups, and domains,"](#) on page 73).
2. Create a new group at the Region level (actually, at any level above the lowest, if you have more than two levels). Call the new group Region01Browsers, because that's what its purpose will be - to allow users from its member groups to browse to their site.

3. Create a similar group for each business entity above the lowest level (Site, in our example).
4. Log on to IBM OpenPages with Watson as a Super Administrator user with the **Access Control Lists** application permission set.
5. Click **Administration > Custom Security**.
6. Navigate to your business entity folder structure (under *|Default|BusinessEntities*).
7. Create an ACL on Region01 and grant Region01Browsers Read access. Repeat this with Region02Browsers in the Region02 business entity folders, and so on in any other Regions you've created.

To make the Browsers groups easy to use, roll-up each site users into a single group that can be added to the Region01Browsers group.

8. Add the R01Site01Directors and R01Site01Writers group to the R01Site01Reviewers group.
9. Add the R01Site01Reviewers group to the Region01Browsers group. This has the effect of adding all of the R01Site01 groups to the Browsers group, even though you only added one.
10. Repeat the process for the rest of the business entities.
11. If you have more than one level above your lowest level, you will need to link the Browsers groups together, creating a chain to the highest level of business entity.

For example, if we had top-level business entities called "Location01," etc., we would create a group called Location01Browsers, and add the Region01Browsers group to it. However, if Region02 was not a child of Location01, you would not add Region02Browsers to the Location01Browsers group.

12. After the groups are added, log out and log back in with a Site level user. Test that the ACLs are working.

Appendix D. Troubleshooting and support for IBM OpenPages with Watson

To isolate and resolve problems with IBM products, use the troubleshooting and support information. This information contains instructions for using the problem-determination resources that are provided with IBM products, including OpenPages with Watson.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and IBM OpenPages Support know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can you reproduce the problem?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution. For more information, see [“Searching knowledge bases” on page 1098](#).

What are the symptoms of the problem?

When you begin to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multisite installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all

corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or were not fully tested together.

When does the problem occur?

Develop a detailed timeline of events that led up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you must look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Even if multiple problems occurred around the same time, the problems are not necessarily related.

Can you reproduce the problem?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can you reproduce the problem on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can you reproduce the problem by running a single command, a set of commands, or a particular application?

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the [IBM Documentation](#). However, sometimes you must look beyond the documentation to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Find the content that you need by using the [IBM Support portal](#).

The IBM Support portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. Go to the IBM Support portal to access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution.

- Search for content by using the IBM masthead search.

You can use the IBM masthead search by typing your search string into the **Search** field at the beginning of any [ibm.com](#)® page.

- Search for content by using any external search engine, such as Google, Yahoo, or Bing.

If you use an external search engine, your results are more likely to include information that is outside the [ibm.com](#) domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on [ibm.com](#).

Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

- Join the IBM Governance, Risk and Compliance (GRC) Community. The IBM GRC Community is a communication forum where IBM can share information about OpenPages with the worldwide community of users. Contact IBM Support for instructions to join.

Getting fixes

A product fix might be available to resolve your problem.

Procedure

To find and install fixes:

- Determine which fix you need. Go to [OpenPages with Watson 8.2 Fix List](#). The Fix List shows a comprehensive list of defect corrections for major releases, fix packs, and interim fixes.
- At the bottom of the Fix List, click the link to the download document for the fix you want to apply.
- Download the fix.
- Apply the fix. Follow the instructions in the "Installation Instructions" section of the download document.
- Subscribe to receive weekly email notifications about fixes and other IBM Support information. For more information, see ["Subscribing to Support notifications"](#) on page 1101.

Contacting IBM Support

IBM Support assists with product defects, answers FAQs, and helps users resolve problems with the product.

Before you begin

After you tried to find your answer or solution by using other self-help options such as Technotes, you can contact IBM Support.

Before you contact IBM Support, your company or organization must have an active IBM maintenance contract, and you must be authorized to submit problems to IBM. For information about the types of

available support, see [Support portfolio](#). For information about how to request access to your company's IBM Support account, see [Requesting access to your company's IBM Support account](#).

About this task

You can open a case from the web, chat, or by phone. For more information, see [Get help with your products](#).

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem.
For more information, see [Getting IBM support](#).
2. Gather the following diagnostic information:
 - Environment type (such as production or development).
 - Application, release, and patch level (such as IBM OpenPages with Watson 8.2.0.1 or IBM OpenPages for IBM Cloud Pak for Data 8.2.2).
 - Description of the issue.
 - Detailed steps to reproduce the issue.
 - Screen captures of the issue.
 - Expected and actual results.
 - OpenPages with Watson log files (for more information, see [Collect logs and diagnostic data](#)).
 - Any workarounds that you have implemented.
 - The date and time that the issue was encountered.
 - Database type and version (such as Oracle 19c or IBM Db2 11.5).
3. Submit the problem to IBM Support in one of the following ways:
 - Online through [IBM Support](#). You can open, update, and view all of your cases from the Service Request portlet on the **Service Request** page. This video demonstrates how to open a case from the IBM Support Community: [Open and manage cases](#).
 - By phone: For the phone number to call in your region, see the [Directory of worldwide contacts](#) web page.

For more information, see [Get help with your products](#).

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

[“Contacting IBM Support” on page 1099](#)

[“Exchanging information with IBM” on page 1100](#)

Exchanging information with IBM

To diagnose or identify a problem, you might be necessary to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Sending information to IBM Support

To reduce the time that is required to resolve your problem, you can send trace and diagnostic information to IBM Support.

About this task

To submit diagnostic information to IBM Support, add the files to your support case. For more information, see [How to Open a Case](#).

Receiving information from IBM Support

Occasionally IBM OpenPages Support might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that IBM OpenPages Support provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that IBM OpenPages Support provided and log in as anonymous. Use your email address as the password.
2. Change to the appropriate directory:
 - a) Change to the `/fromibm` directory.

```
cd fromibm
```

- b) Change to the directory that IBM OpenPages Support provided.

```
cd nameofdirectory
```

3. Enable binary mode for your session.

```
binary
```

4. Use the **get** command to download the file that IBM OpenPages Support specified.

```
get filename.extension
```

5. End your FTP session.

```
quit
```

Subscribing to Support notifications

To stay informed of important information about the IBM products that you use, you can subscribe to notifications.

About this task

By subscribing to receive notifications about IBM OpenPages with Watson or IBM OpenPages for IBM Cloud Pak for Data, you can receive important technical information and updates for specific IBM Support tools and resources.

Procedure

1. Go to the [IBM Support portal](#).

2. Sign in using your IBM ID and password.
3. Click the person icon and select **Settings**.
4. Expand **Case notification settings** and select the options you prefer.

Known problems and solutions for global search

Issues that are related to the IBM OpenPages with Watson global search component are most commonly encountered when you are setting it up or when it is updated to synchronize the search index for changes that are made to the OpenPages with Watson schema (such as adding or removing object types or fields).

When an administrative operation fails, you can normally resolve these issues by clicking **View Log** to see the log message for the failed global search operation.

The most common failure is that the search service is not started, for which you see this error:

"Could not establish connection to the search engine. Please contact your system administrator."

Ensure that the search service is started or restart to try to resolve the issue.

Global search start fails

If you configured the global search services to start and stop by using a script and you forgot to stop global search before rebooting the system, when you attempt to start the global search services, the services will fail to start. To fix this issue complete the following steps.

Procedure

1. Log on to the search server as a user with administrative privileges.
2. Open a command line on the search server.
3. Go to the `<SEARCH_HOME>/opsearchtools/` directory and run the following commands.

On Microsoft Windows operating systems, run:

```
opsearchtool.cmd clearState -indexname openpages
opsearchtool.cmd clearState -indexname folderacl
```

On Linux operating systems, run:

```
./opsearchtool.sh clearState -indexname openpages
./opsearchtool.sh clearState -indexname folderacl
```

Global search setup fails

In some rare cases, the global search component might encounter a failure during the creation of the search index, before the operation completes. The failure might be caused by hardware issues, database issues, or a power outage, for example. When this happens, the state of the global search setup is in an undefined state and the **Enable** button might become available, giving the misleading impression that global search was set up successfully. To recover from this state, investigate the root cause, resolve it, and then set up global search again.

Procedure

1. Investigate and resolve the root cause of the failure.
2. Log on to OpenPages as a user with administrative privileges.
3. Click **Administration > Global Search**.
4. Click **Drop** to drop the search index.
5. Wait for the drop process to complete.

If the **Drop** button is not available or if the drop process fails, see [“Forcing a reset of global search” on page 1103](#).

6. Click **Create** to re-create the search index.

Forcing a reset of global search

In some rare cases, it might be necessary to reset the IBM OpenPages with Watson global search component if you cannot restore it from the **Global Search** administration page. These issues might prevent you from successfully completing tasks in the global search administration page. To resolve these issues, complete the following steps.

Procedure

1. If you started a global search indexing process from the OpenPages user interface, click **Administration > Global Search**. Make a note of the **Id** of the indexing process. You need the **Id** in step “9” on page 1104.
2. Log on to the search server as a user with administrative privileges.
3. Open a command line on the search server.
4. Go to the <SEARCH_HOME>/opsearchtools/ directory to run the commands in the following steps.



Attention: At the successful completion of each command, the statement "Normal completion of command" should appear. If it does not, contact Customer Support to diagnose the issue.

5. Ensure that Solr is running and is reachable on port 8983. If Solr is not running, then run the following command to start it.

Microsoft Windows:

```
opsearchtool.cmd startSolr
```

Linux:

```
./opsearchtool.sh startSolr
```

6. Run the following commands to stop indexing.

Microsoft Windows:

```
opsearchtool.cmd stopIndexing -indexname openpages  
opsearchtool.cmd stopIndexing -indexname folderacl
```

Linux:

```
./opsearchtool.sh stopIndexing -indexname openpages  
./opsearchtool.sh stopIndexing -indexname folderacl
```

7. Verify that no opsearchtool.jar processes are running.

On Microsoft Windows operating systems, use the task manager to see whether any opsearchtool.jar processes are running. If there are, terminate them.

On Linux operating systems, use the ps command to see whether any opsearchtool.jar processes are running. If there are, terminate them.

8. Run the following commands to clear any PID states that might still be set if the opsearchtool.jar processes did not end successfully.

Microsoft Windows:

```
opsearchtool.cmd clearState -indexname openpages  
opsearchtool.cmd clearState -indexname folderacl
```

Linux:

```
./opsearchtool.sh clearState -indexname openpages  
./opsearchtool.sh clearState -indexname folderacl
```

9. If a global search indexing process was started from the OpenPages user interface, run the following commands:

Replace %lrpf-pid% with the **Id** of the indexing process.

Microsoft Windows:

```
opsearchtool.cmd syncIndex -terminatepid %lrpf-pid%  
opsearchtool.cmd fullIndex -indexname openpages -terminatepid %lrpf-pid%  
opsearchtool.cmd fullIndex -indexname folderacl -terminatepid %lrpf-pid%
```

Linux:

```
./opsearchtool.sh syncIndex -terminatepid %lrpf-pid%  
./opsearchtool.sh fullIndex -indexname openpages -terminatepid %lrpf-pid%  
./opsearchtool.sh fullIndex -indexname folderacl -terminatepid %lrpf-pid%
```

10. Run the following commands to reset global search.

Microsoft Windows:

```
opsearchtool.cmd resetSolr -indexname openpages  
opsearchtool.cmd resetSolr -indexname folderacl  
opsearchtool.cmd resetDb  
opsearchtool.cmd stopSolr  
opsearchtool.cmd startSolr
```

Linux:

```
./opsearchtool.sh resetSolr -indexname openpages  
./opsearchtool.sh resetSolr -indexname folderacl  
./opsearchtool.sh resetDb  
./opsearchtool.sh stopSolr  
./opsearchtool.sh startSolr
```

11. Log on to OpenPages as a user with administrative privileges.
12. Click **Administration > Global Search**.
13. Click **Create** to re-create the search index.

What to do next

Resetting the global search component does not change your global search settings, such as object types, fields that are enabled for search, registry settings, or property settings. The reset disables the global search component. You must enable it again to make it available to users.

Checking for global search setup issues and periodic monitoring

When the incremental indexer is running during global search setup or after setup, some records might not get indexed due to issues with the record, other system errors, or application errors.

About this task

If the issues are not unrecoverable, they do not impede the setup process or the incremental indexer. However, the records that do not get indexed are logged in an error-log file, with an error message that explains the issue so you can take appropriate action. The error-log files are never rotated. Periodically examine this directory for new error files.

Procedure

1. Log on to OpenPages as a user with administrative privileges.

2. Go to the directory <SEARCH_HOME>/opsearchtools/logs_error/ .
3. Examine this directory for new error files.

Before you contact IBM OpenPages Support

When you contact IBM OpenPages Support, you need to collect diagnostic data and provide a detailed use case of the issue.

About this task

Before you contact IBM OpenPages Support to help with resolving global search issues, follow these steps to collect diagnostic data.

Note: You do not need to stop global search, the OpenPages application server, the database server, or any other application when you run the **collectDiagData** command.

Procedure

1. Log in to the OpenPages global search server as a user with administrative privileges.
2. Open a command prompt or a shell window.
3. Go to the <SEARCH_HOME>/opsearchtools/ folder and run the following commands:

- Microsoft Windows:

```
mkdir diag
opsearchtool.cmd collectDiagData -diagpath diag
```

- Linux:

```
mkdir diag
./opsearchtool.sh collectDiagData -diagpath diag
```



Attention: The **collectDiagData** command might report warning messages that look as if the command failed. This warning can happen due to a number of reasons, such as the data that is being collected cannot be accessed or is not yet available. If you see any such warnings, capture them and include them as part of the diagnostic data to IBM OpenPages Support.

4. Add the contents of the new folder that is created under the diag folder to a compressed file.
5. Send the compressed file and complete details about your issue to IBM OpenPages Support.

Known problems and solutions for the QRadar integration package

Some common problems with QRadar integration package are documented, along with their solutions or workarounds. If you have a problem with QRadar integration package, review the problem-solution topics to determine whether a solution is available to the problem that you are experiencing.

SDI properties file error message

When you run the assembly line in the qradar_integration project, you might see one or more warning messages with the error code CTGDIR103W in the IBM Security Directory Integrator (SDI) console.

This message indicates that the enclosing project is missing a properties file, and that the file will be created if anything is written to it.

The following text is an example of a warning that might appear when you run any of the assembly lines that are contained in the qradar_integration project that is included with IBM OpenPages with Watson:

```
Wed Aug 19 11:13:35 EDT 2015 [qradar_integration] WARN - CTGDIR103W
The properties file 'C:/SDI-Solutions/workspace/qradar_integration/Runtime-qradar_integration/
```

`gradar_integration.properties'`
for `Properties.gradar_integration` was not found, and will be created if anything is written to it.

These warnings can be safely ignored. In general, a Security Directory Integrator project typically has an associated properties file named after the enclosing project to hold any project-specific properties, but this file is not strictly required.

Do not include security domain groups when creating object filters or security rule formulas

When creating filters for object types using the **Administration > Object Types** pages or security rule formulas that involve fields permitting user group selection, it is possible to select a security domain group because these groups are included in the selection list. The selection will not be flagged as an error. However, if you include a security domain group in the object filter criteria or in the security rule, you might encounter application errors later.

To avoid potential errors, ensure that you select a valid user group, and not a security domain group. In

the product user interface, security domain groups are represented by this icon , and user groups are

represented by this icon .

Objects can be saved with an empty required field

If an object contains a redacted field that is also a required field, a user can successfully save the object even when the redacted field value is empty in the OpenPages repository.

JSON file might not display multibyte characters correctly in Wordpad

When you export a JSON file for a Dashboard tab configuration and open it in Microsoft Wordpad, multibyte characters might be corrupted.

This issue might occur if you go to **Administration > Profiles**, select a Dashboard tab that uses multibyte characters, click **Edit** and then click **Export JSON**. If you select Wordpad as the application to open the file, the multibyte characters might not display correctly.

The solution is to open JSON files in a text editor that supports UTF-8. The JSON file will display correctly in Notepad or Microsoft Word.

Remediating after an Enumerated String field is changed to a multi-select field (Db2)

If you are using IBM Db2, a subsequent maintenance task is required whenever you convert an enumerated string from single to multi-select. You do not need to do this task immediately. Do this task during your next available maintenance window.

About this task

After an enumerated string field is changed to multi-select, the associated reporting schema tables in the OpenPages database will contain obsolete columns. The application handles the presence of these columns, but a subsequent cleanup should be scheduled in the next available maintenance window. If left unmanaged, these obsolete columns might eventually cause errors in OpenPages.

You can resolve the issue by running a utility against the Db2 database. Alternatively, you can drop and re-create the reporting schema to resolve the issue.

Procedure

1. Log on to the OpenPages admin application server as a user with administrative privileges.
2. Stop all OpenPages services.
3. If you are using Microsoft Windows, start the Db2 command line processor by typing db2cmd.
4. Log in to CLPPLUS as the OpenPages database user, for example openpages.
5. Run the following command:

```
call OP_RPS_MGR.DROP_AND_REORG_OBSOLETE_RT_COLS;
```

The length of time that it takes for the command to run varies depending on the number of tables with obsolete columns that need to be dropped and the size of those tables.

When the command completes, the following message is displayed:

```
DB250000I: The command completed successfully.
```

System delay when modifying object types and fields (Db2)

If you are using IBM Db2 and the reporting schema is enabled, you can encounter a significant system delay in OpenPages if you make object model modifications. The delay is due to locking conflicts on the IBM Db2 platform.

The following object model modifications can cause a system delay:

- Associating a field group to an object type
- Adding a new field to a field group that is already associated to an object type
- Converting a single valued enumerated field to a multi-valued enumerated field
- Adding new object type associations

To reduce a system delay, follow this process:

1. Choose a time when there is limited or no activity on the system.
2. Enable System Admin Mode.
3. Shut down Cognos Analytics.
4. Disable global search.
5. Complete the object model modifications.
6. Start Cognos Analytics.
7. Enable global search.

Object model modifications cause implicit DDL operations to be performed against the reporting schema. On the IBM Db2 platform share locks are automatically acquired when a read operation is performed. A read operation can block the object model modification. If the read operation is long running, for example, a long running Cognos report, the object model modification can appear to hang. In reality, the object model modification is not hanging but blocked on the session that is performing the read operation. After the read operation completes, the session that is attempting the object modification can proceed. The read operation needs to complete and clear its locks before the implicit DDL operation can acquire the locks that it needs to implement the object model change. If you kill the object model modification operation, the system can be left in an inconsistent state. If this happens, you must recreate the reporting schema.

The following actions do not cause this issue:

- Creating a new object type
- Creating a new field group
- Adding fields to a field group that is not yet associated to an object type

- Changing object text values
- Switching a field from not required to required or vice versa
- Changing the order of enumerated strings in an enumerated field
- Hiding an enumerated field value
- Adding new values to an existing enumerated field
- Modifying profile definitions
- Creating new reporting periods
- Enabling or disabling existing object type associations
- Enabling or disabling of security rules
- Enabling or disabling field level encryption

NoClassDefFoundError errors when you run custom code

If you have custom deliverables, such as a JAR file or JSP, that uses third-party APIs, you might see a `NoClassDefFoundError` error. The error happens because Liberty does not enable third-party APIs by default. You need to enable access to third-party APIs.

To resolve the error, edit the `apiTypeVisibility` attribute in the `<OP_HOME>/wlp-user/servers/<server_name>Server</server_name>/configDropins/overrides/op-apps.xml` file. For example:

```
<classloader id="opappClassLoader" apiTypeVisibility="+third-party" commonLibraryRef="jaas-proxy" privateLibraryRef="ext-lib" />
```

For more information, see [Accessing third-party APIs from a Java EE application](#) in the Liberty documentation.

Risk Assessment Summary report does not show related risks and controls

The **Risk Assessment Reports > Risk Assessment Summary** report does not show related risks and controls.

This issue can occur when you use the object relationship **Risk Assessment > Process > Risk > Control**.

To resolve the issue, update the `OPENPAGES_REPORTS_V6` reporting framework, and then regenerate the framework.

1. In the Task Focused UI, click  > **System Configuration > Settings**.
2. Go to **Platform > Reporting Framework V6 > Models > OPENPAGES_FRAMEWORK_V6 > Namespaces > RA1 > Object Model**.
3. In the **Value** field, add the following to the end of the value:

```
,RiskAssessment|SOXProcess,SOXProcess|SOXRisk
```

4. Click **Done**.
5. Regenerate the reporting framework. For more information, see [“Updating the reporting framework \(Task Focused UI\)”](#) on page 977.
6. Open the Risk Assessment Summary report. The report now displays risks and controls that are associated with the risk assessment.

Troubleshooting helpers

If you encounter a problem with a helper, you can configure registry settings to create logs for the helper.

For more information, see in the Solutions Guide.

Appendix E. Best practices for configuring IBM OpenPages with Watson

To improve the performance of IBM OpenPages with Watson, administrators can design, configure, and implement OpenPages with Watson applications using best practices. These suggested guidelines are provided to help you maximize, streamline, and get the most out of the product environment.

Use short field names and field group names

When creating field groups and field names, use short field group names and short field names.

The length of field group names and field names have the following impacts:

- Long names restrict the number of fields that you can have on an object type.
- Long names increase the length of object type user defined attributes (UDAs), which have a 64 character maximum.

After creating the short field group names and short field names, an administrator can relabel and localize the field names to add meaning. For example, an administrator might create a field called `AudDesEff`, which can be difficult for a user to interpret. In the **Object Text** area of the application, the administrator can update the locale and change the label to a more meaningful name, such as `Audit Design Effectiveness`. By doing this, the administrator minimizes the length of the name but also retains a positive user experience.

Be aware that Java applets are not supported by the Chrome browser

Some functionality that depends on Java applets, such as the File Upload, may not work as expected when you use the Chrome browser.

Because the Chrome browser does not support Java applets, the Optimized File Upload button on the detail page does not show on browsers that don't support it. For more information, see [“Optimize file uploads”](#) on page 613.

Limit the number of objects in views

The IBM OpenPages with Watson application allows end users to access data in various views (such as the Overview, Folder Views, Filtered List View, Detail View, Activity Views, and so on). Limiting the number of objects that are displayed in a view improves performance.

About this task

Limit the number of objects in a particular folder location to no more than 150 or 200 objects. If a folder location has more than 200 objects, end users may see performance issues when expanding the folder location, depending on how fast the server is and how fast the browser is.

Limit the number of associations in the Overview

Limit the number of child associations for objects in the **Overview** screen to improve load time for this view.

About this task

Unlike the other views, the **Overview** screen shows objects by associations. If an object has numerous child associations, the page will take longer to display all the content. Administrators can limit the type of child associations displayed by editing the profile and removing various object types.

Procedure

1. Open a supported browser.
2. Go to the IBM OpenPages with Watson URL.
3. Log in with an administrator ID.
4. On the navigation menu bar, click **Administration > Profiles**.
5. Click a profile.
6. In the **Object Types** section, click the object type.
7. Scroll to the **Navigational Views** section.
8. Click on the **Overview** link.
9. In the **Included Object Types** section, modify the list accordingly.

Limit the number of portlets on the home page

In IBM OpenPages with Watson, you can configure portlets on the home page that contain predefined tables or embedded reports. Each portlet that you add to a tab on the home page increases the work that is required to display that tab. A large number of portlets per tab can negatively impact performance. Therefore, you should limit the number of portlets on the home page.

About this task

The exact cost to fetch and display the data for each portlet depends on a number of factors, for example, the data size, filter criteria, security rules, browser, and available system resources.

Limit activity views with field dependencies and dependent picklists

In dependent picklists, the more fields in the picklist, the more JavaScript is required to display the object to users.

In IBM OpenPages with Watson, administrators can create user views within a profile. Administrators can also create dynamic field dependencies and dynamic dependent picklists. Depending on how the business object model was designed, a picklist could have several dozen fields as selectable items. Javascript is used to control this behavior when an end user renders the field. The more field dependencies and dependent picklists that are created for an object type, the more javascript is required for an end user to view the object. Depending on what browser is utilized, this can cause performance issues in rendering the page.

When combined with an activity view, an end user can list multiple objects at once. When multiple objects are displayed (such as a 3-level activity view), it will increase the amount of javascript that is loaded on the page.

Limit the number of security rules and complexity of security rules

As an OpenPages administrator, you can use Field Level Security (FLS) and Record Level Security (RLS) in the IBM OpenPages with Watson application to create another level of robustness for implementing security.

You can use the rule engine to implement a variety of business security options. With this flexibility, remember that the more complex the rule, the more time it will take to evaluate the rule. The same is also true for the number of rules that are being implemented.

In other words, security rules and evaluating security rules adds a level of overhead to end user operations. End user operations include but are not limited to tasks such as updating an object, using the bulk update in a grid view, and filtering through data.

Limit the number of SOXBusEntity objects in the system

The SOXBusEntity object type is a special object type. When an OpenPages power user or OpenPages administrator creates a SOXBusEntity object type in the IBM OpenPages with Watson application, an additional overhead is associated with it.

For example, it might create an additional security context point for OpenPages administrators. This creates additional administrative overhead for administrators. Additionally, adding additional SOXBusEntity object types also adds additional load to the security cache engine.

Be aware of shared field groups

When using a field group that is shared amongst other object types, the administrator should be aware that a small change in that field group will have an effect on all the object types using it.

The IBM OpenPages with Watson application allows an object type to use multiple field groups. These field groups can also be used by other object types.

If an administrator adds one or two fields to the shared field group, those one or two fields will now also be associated with the object types that are using it. If one of the other object types is near the dynamic reporting schema SQL limitation of 32,000, it may cause problems regenerating the reporting schema.

Eliminating unused object type relationships

If the business only requires a subset of the available enabled relationships, those unneeded relationships should be disabled.

About this task

When you install the IBM OpenPages with Watson solutions, it loads dozens of object types and hundreds of parent-child relationships. Depending on your business needs, your business object model may only use a small subset of the object types and a subset of the parent-child relationships.

Disabling unused object types will prevent any accidental creations of those relationships.

With Oracle databases, one method of analyzing if there are any unused and enabled relationships is to run an SQL script. From the installation media, there are folders that contain SQL scripts. One of the SQL scripts within the folder is: `Analyze-Object-Type-Relations.sql`.

For IBM Db2 information, see the [IBM Db2 documentation](#).

Procedure

1. Log on to SQL*Plus as the OPENPAGES oracle id.
2. Type the following command to allow the output to occur: `SET SERVEROUTPUT ON;`
3. Type the following to spool the contents to a log: `SPPOOL AnalyzeRelationships.txt;`
4. Run the script by typing `@Analyze-Object-Type-Relations.sql`.
5. Run the following to stop the spooling of the log: `SPPOOL OFF; .`

The log file will identify any relationships that are enabled in the system but there are no instances of data utilizing those relationships.

Displaying reporting fragments only on demand

These reporting fragments can be displayed automatically when an end user views the page or on-demand when a user explicitly would like to see the reporting fragment. Set reporting fragments to display only on demand to improve performance of the Cognos server and database instance.

About this task

A reporting fragment is a metadata type that is configured with the administrative screens. It allows an administrator to display Cognos objects within the context of an IBM OpenPages with Watson object. Cognos objects can be anything from a simple list to a graph object. Where fragments are unlikely to be necessary, set reporting fragments to display On Demand.

By setting reporting fragments to display on-demand, it reduces excessive calls to the Cognos reporting server. Depending on how complex the design of the reporting fragment is, this can greatly reduce overhead to the Cognos server and to the database instance.

Procedure

1. Open a supported browser.
2. Go to the OpenPages with Watson URL.
3. Log in with an administrator ID.
4. On the navigation menu bar, click **Administration > Profiles**.
5. Click a profile.
6. In the **Object Types** section, click the name of the object type using the display.
7. In the **Object Fields** table for the selected object type, click the name of the reporting fragment to open its details page.
8. In the **Object Field Information** section, click **Edit**.
9. Update the **Display Type** dropdown.

Displaying Cognos reports on home page tabs

IBM OpenPages with Watson administrators can configure Cognos reports to display on the home page tabs instead of on the My Work home page.

About this task

OpenPages with Watson administrators can configure the My Work home page to display reports on-demand, configure the My Work home page to display a list of reports, and have users click on tabs to run reports on request.

When the administrator configures the home page to display reports on the tabbed home page, the reports run only when the user specifically wants to view the report. This configuration reduces excessive load and traffic to the IBM Cognos reporting server. When reports are configured to run on demand on the My Work home page, OpenPages with Watson users might not even use the data returned from the report. At times, if the My Work home page is configured to display multiple Cognos reports on demand, the portlets might not display properly, forcing users to refresh the home page.

Procedure

1. Open a supported browser.
2. Go to the OpenPages with Watson URL.
3. Log in with an administrator ID.
4. On the navigation menu bar, click **Administration > Profiles**.
5. Click a profile.

6. Use the **Home Page Tab Configuration** section to display reports on various tabs or the **My Work Tab Configuration** area to display reports on the My Work home page.

Setting a minimal starting group for display types

IBM OpenPages with Watson administrators can change the starting groups for display types to minimize the number of users that are initially displayed.

About this task

OpenPages with Watson profiles have various configurable display types. Display types, including user selector, multiple user selector, user dropdown, user/group selector, multiple user/group selector, group selector, and multiple group selector can be minimized. Select a starting group that minimizes the amount of users and/or groups returned by the display type but still has the appropriate business value. By minimizing the starting group, you reduce the number of users that the end user has to search through.

Procedure

1. Open a supported browser.
2. Go to the OpenPages with Watson URL.
3. Log in with an administrator ID.
4. On the navigation menu bar, click **Administration > Profiles**.
5. Click a profile.
6. In the **Object Types** section, click the name of the object type using the display.
7. In the **Object Fields** table for the selected object type, click the name of the field using one of the display types to open its details page.
8. In the **Display Type Information** section, click **Edit**.
9. Update the **Starting Group** value.

Task-oriented hyperlinking

You can add hyperlinks that are directly oriented to user tasks, from internal or external locations to IBM OpenPages with Watson views. These hyperlinks can also include filters.

For example, in a notification email to a risk owner, you can include a hyperlink to the Filtered List View for Risks with the **Risks Awaiting Assessment** filter added to the link.

You can create hyperlinks that include the following target views:

- The Detail View for a specific object instance, in read-only mode.
- A specific activity view for an object instance.
- The Filtered List View for a specific object type with a public filter applied.
- A specific grid view for an object type with a public filter applied.
- Add New wizard within the OpenPages application. The wizard opens in its own browser tab instead of a pop-up, even if the user was logged in to OpenPages when they clicked the link.

You can add hyperlinks to the following locations:

- OpenPages Reports.
- Notification emails.
- OpenPages Java Server Page (.jsp) file type helper applications.
- Within the OpenPages application, using computed fields or URL link fields.

The following sample URLs can help you create task-oriented hyperlinks:

- In the samples the URLs are created by using either the name value, or the resource ID value for views, objects, and filters.

- If you use a name for a value, replace any spaces in the name with the characters %20. URLs cannot contain spaces.
- If you use a fileId, viewId, or filterId to create a URL, the values for the Ids are the resource IDs of specific object instances, views, or filters.
- There is one Filtered List View, but many possible Grid Views. There is one Detail View, but many possible Activity Views.
- For the Add New wizard hyperlinks you can combine the parameters in more ways than are described in the samples. For example, you can specify a parent without specifying a view.

To Filtered List View with the object type, grid view, and filter specified

Syntax:

/openpages/app/jspview/flv?prmt=<name of the object type>&view=<name of the grid view>&filter=<name of the public filter>

Example:

/openpages/app/jspview/flv?prmt=SOXProcess&view=PRSA%20Update&filter=My%20Processes

To Filtered List View with the object type, Filtered List View, and filter specified

Syntax:

/openpages/app/jspview/flv?prmt=<name of the object type>&view=Filtered%20List&filter=<name of the public filter>

Example:

/openpages/app/jspview/flv?prmt=SOXProcess &view=Filtered%20List&filter=My%20Processes

To Filtered List View or Grid View with the object type, view, and filter specified

Syntax:

In this example, the values are resource IDs instead of names.

Example:

/openpages/app/jspview/flv?prmtId=97&viewId=205&filterId=101

To Filtered List View with the object type and view specified (previous filter is applied)

Syntax:

When a filter is not specified, the most recent, previously used filter is applied. The view, and filter parameters are optional.

Examples:

/openpages/app/jspview/flv?prmt=SOXProcess&view=PRSA%20Update

/openpages/app/jspview/flv?prmtId=97&viewId=205

To Filtered List View or Grid View, object type specified (previous view and filter are applied)

Example:

/openpages/app/jspview/flv?prmt=SOXProcess

To Detail View or Activity View

Syntax:

In the following examples, the fileId value is expressed by using the *<resource ID for the specific object instance>*, while the view value is expressed by using either the view ID, or the *<name of the view>*.

/openpages/view.resource.do?fileId=<resource ID for the specific object instance>&view=<name of the view, which can be Detail, OR the name of one of the specific activity views>

Examples:

/openpages/view.resource.do?fileId=1903&view=Control%20Assessment

/openpages/view.resource.do?fileId=1903&view=Detail

/openpages/view.resource.do?fileId=1903&viewId=20

To Add New wizard with only the object type specified

Syntax:

/openpages/app/jspview/addNew?objectType=<name of object type>

or

/openpages/app/jspview/addNew?objectTypeId=<id of object type>

Examples:

/openpages/app/jspview/addNew?objectType=SOXControl

/openpages/app/jspview/addNew?objectTypeId=40

Object type or object type ID is required in a URL that opens the Add New wizard. It is likely that you would use object type ID only if the URL is generated and the object type id is conveniently available.

To Add New wizard with object type and view specified

Syntax:

/openpages/app/jspview/addNew?objectType=<name of the object type>&viewName=<name of the view>

Example:

/openpages/app/jspview/addNew?objectType=SOXControl&viewName=ShortViewForControl

or

/openpages/app/jspview/addNew?objectType=SOXControl&viewId=3247

View name or ID is optional. If you provide it, it determines the layout of the Add New wizard. You can choose any Creation view or Object View. If you use an Object view with multiple levels of objects, any non-direct children on the second level and all descendants on the third level is ignored. Direct children are used to populate an Associate page in the wizard to enable the associating of children at the same time the object is created.

If no view is specified or the specified view is invalid or disabled, the default Creation view is used. If there is more than one Creation view, the user is prompted to select one.

If there are no Creation views, the Detail view is used.

If the Detail view is disabled or does not exist, the default Object view is used.

For more information about creation views see [“Creation views”](#) on page 327.

To Add New wizard with object type, view, and parent object type specified

Syntax:

/openpages/app/jspview/addNew?objectType=<name of the object type>&viewName=<name of the view>&parentObjType=<name of the parent object type>

or

/openpages/app/jspview/addNew?objectType=<name of the object type>&viewName=<name of the view>&parentObjTypeId=<id of the parent object type>

Example:

/openpages/app/jspview/addNew?
objectType=SOXControl&viewName=ShortViewForControl&parentObjTypeId=11

Parent object type or parent object type ID is optional. If multiple object types are suitable as parents for this object type, the default is the one specified in the setting Applications/GRCM/Add New Wizard/Parent Object Type Preferences. If the specified parent object type is invalid, it is ignored.

It is likely that you would use parent type ID only if the URL is generated and the object type id is conveniently available.

To Add New wizard with object type, view, and parent specified

Syntax:

`/openpages/app/jspview/addNew?objectType=<name of the object type>&viewName=<name of the view>&parentObjType=<name of the parent object type>&parentObjId=<id of the parent object >`

Example:

`/openpages/app/jspview/addNew?
objectType=SOXControl&viewName=ShortViewForControl&parentObjType=SOXRisk&parentObjId=1234`

Parent object ID is optional. Use this parameter to pre-select the parent on the Parents page of the wizard. If specified, the parent object type is required. If you are not creating the URL programmatically, you can find the parentObjId by navigating to the object in the Detail page and using the prmId parameter. If the specified parent object is invalid, it is ignored.

Appendix F. Creating custom actions for GRC workflows

You can create custom actions to use in IBM OpenPages with Watson workflows.

A custom action is a Java class that can be invoked during a workflow action. A custom action is very similar in function to a trigger, which executes on object operations. But triggers and custom actions have different interfaces and abstract implementations, so the classes are not interchangeable. Like triggers, custom actions must be deployed to each OpenPages application server and are dynamically loaded during startup.

To implement a custom action, do the following tasks:

- Create a custom action Java class by extending the abstract implementation `com.ibm.openpages.api.workflow.actions.AbstractCustomAction`
- Add the class to a JAR file. Use the JAR file for all of your custom code. Deploy the JAR file to each OpenPages application server in the `<OP_HOME>/aurora/op-ext-lib` directory.
- Restart the OpenPages application servers so that the custom action can be picked up by the dynamic class loader.
- Configure the custom action within the context of a workflow by using the **Custom Action** operation type. Set any property values or fields that the custom action requires as inputs.

Custom actions run in the order of operation that is listed in the workflow action.

All operations in a workflow action are performed in a single transaction. This means that if a custom action fails for any reason, the entire workflow action is rolled back.

Passing arguments to a custom action

In order for the custom actions to be reusable in different contexts, properties and field values can be passed in during configuration. This is optional. As the developer of the custom action class, you decide which, if any, arguments to pass in and validate.

- Properties are name-value pairs that you define. For example, you might create a custom action that creates a child object and has a property that is named `object_type` that determines the type of object to create.
 - The custom action needs to validate that the properties that it expects to be passed in have been passed in and that they have valid values.
 - You can use expressions, such as `[$END_USER$]` or `[$TODAY$]` in the property values to pass in dynamic content. For a full list of expressions, see [“Using variables, functions, and fields” on page 503](#).
- Fields can also be passed in to provide a typed value to an object field. This technique can be very useful if your custom action is interacting with objects, either setting or evaluating field values.

Authoring the custom action Java class

The only requirement of a custom action Java class is that it extends `com.ibm.openpages.api.workflow.actions.AbstractCustomAction`. This requirement is validated when the custom action is defined in a workflow.

A single abstract API must be implemented in `AbstractCustomAction`:

```
process();
```

Use this method to contain the business logic that the custom action will perform.

For information about the OpenPages GRC API, which you can use in custom actions, see the *IBM OpenPages with Watson API Javadoc*. For links to the Javadoc, see [Appendix G, “OpenPages API documentation,”](#) on page 1121.

You can access context about the current workflow and configuration through the following methods on `AbstractCustomAction`:

- `getContext()` – Returns an `IWFOperationContext` object that contains all relevant information about the workflow state and the associated `GRCObject`.
- `getPropertyValue(String prop_name)` – Returns the value of a named property.
- `getFields()` – Returns a `List<IWFFieldSetter>` object based on the configuration of the custom action.

Exception or validation messages can be thrown from a custom action and displayed to the user. To display messages, use:

```
throwException(String message, Throwable cause)
```

Use this method to throw exceptions and display a custom message to users. Uncaught exceptions or exceptions that are explicitly thrown are logged by the application, but only a general error message is displayed to users.

Workflow context

The class `com.ibm.openpages.api.workflow.actions.IWFOperationContext` provides state information for the workflow action.

Related workflow data:

- `IWFProcessDefinition` `getProcessDefinition()` – Returns the workflow definition.
- `IWFProcess` `getProcess()` – Returns the current workflow instance.
- `IWFActivityInstance` `getActivityInstance()` – Returns the current stage instance.
- `IWFTransition` `getTransition()` – Returns the current workflow action.

Related `GRCObject`:

- `IGRCObject` `getResource()` – Returns the `GRCObject` for the workflow instance.
- `Id` `getResourceId()` – Returns the ID of the `GRCObject`.

Service API access:

- `IServiceFactory` `getServiceFactory()` – Returns a service factory for instantiating other OpenPages GRC API services.

Tips

- Updating objects:

If you want your custom action to update an object for the current workflow action, access the object through `IWFOperationContext.getResource()`. Updates that are made in this way are saved automatically by the workflow engine. Use this technique so that changes by multiple operations during an action are saved only once.

If your custom action looks up other objects and modifies them, the custom action must save the objects explicitly. You can save the changes by using `IResourceService.saveResource()`. For example, if your custom action updates controls that are children of a risk, save the controls explicitly.

- Utility functions:

The class `com.ibm.openpages.api.workflow.actions.util.WFActionUtil` has some useful utility functions that you can use in a custom action. Review the *IBM OpenPages with Watson API Javadoc* for a full list of functions.

Examples:

- `replaceStringExpressions(IWFOperationContext context, String value)` – This function takes any string value and replaces expressions in it. This function is very useful if you want to leverage expressions in property values that are passed in to your custom actions.
- `setFieldValue(IWFOperationContext context, IGRCObject grcObject, IWFFieldSetter field)` – This function updates the object with the field setter value that is passed in. This field can also use expressions in its value.

Appendix G. OpenPages API documentation

For information about IBM OpenPages with Watson APIs, see the following documentation.

- [OpenPages with Watson API OpenAPI Reference \(HTML\)](#)
- [OpenPages with Watson API Javadoc \(HTML\)](#)
- [OpenPages GRC REST API Reference Guide \(.pdf file\)](#)
- [OpenPages with Watson SDK REST Samples \(.zip file\)](#)

Appendix H. Personal information processed and stored by OpenPages

IBM OpenPages with Watson stores certain personal information (PI). The personal information is stored in the OpenPages repository, specifically in the OpenPages database.

OpenPages stores and processes the following basic personal information:

- User name
- First name (given name)
- Last name (surname)
- Email address

For more information, see [Chapter 4, “Users, groups, and domains,” on page 73.](#)

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. This document may describe products, services, or features that are not included in the Program or license entitlement that you have purchased.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Location Code FTO
550 King Street
Littleton, MA

01460-1250
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

Copyright

Licensed Materials - Property of IBM Corporation.

© Copyright IBM Corporation, 2003, 2023.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written.

These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at ["Copyright and trademark information."](#)

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

The registered trademark Linux is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat, JBoss®, OpenShift, Fedora®, Hibernate®, Ansible®, CloudForm, RHCA®, RHCE®, RHCSA®, Ceph®, and Gluster® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.



Glossary

In this glossary, you can find terms and definitions for IBM OpenPages with Watson

access control list (ACL)

A concept in computer security used to determine the permissions (Read, Write, Delete, and Associate) a user or group can have on the folder structure of an object type (such as, an Entity, Risk, or Test). ACLs provide a means to control who has access to what and with which permissions. ACLs can be assigned to groups and users via a role template.

Action menu

The menu that is displayed in views. Your permissions determine which menus and items are available.

Actor ACLs

These are a set of administrator access rights (Manage, Lock, Unlock, Reset Passwords, Assign Roles, Browse) defined on users and groups. These access rights control the operations an administrator can perform on a particular user or group.

administrator

A user that is granted special permission to manage a Business Entity, including the assignment of Roles to users and groups.

application permissions

A list of permissions that allow groups and users to access certain activities, including administration, within the application (such as the ability to view, lock, or unlock objects, or create and delete reporting periods).

associations

Relationships that exist among objects, or between objects and attached files. Example: A sub-entity may be directly associated with a process or business function.

audit universe

The aggregate of all areas within an organization that can be audited.

business unit

One or more Entities, Processes, or Sub-Processes.

CSV

Comma separated values. A type of file that uses a comma-delimited format.

group

A generic term that encompasses both organizational and security domain groups.

listing pane

The pane on an object's Detail View page that is displayed when you click the name of an associated object type. It lists all the names of objects for that type that are associated with the current object, and has an Actions Menu for adding new objects, or associating and copying existing objects of the same type.

object

Any item that contains or receives information, such as Business Entities, Processes, Risks, Controls, Issues, Tests and so forth. In a security context, an object is the piece of data to which access control is applied (such as, Business Entity, Process, Sub Process, Risk Assessment). Also called "resource".

object type

A category or type of object, such as a Risks, Controls, Issues and so forth. In a hierarchy of objects, each object type has a set of allowed relationships with other object types.

organizational group

A group that is created by an administrator to organize users within an organization. Organizational groups are typically associated with security domain groups and other organizational groups.

pane

A section or component of an object view. For example, a Detail View page typically consists of several panes, such as a Details pane, Context pane, Associations pane, Listing pane, and an Attachments pane.

resource

See "object".

Resource ACLs

These are a set of access rights (Read, Write, Delete and Associate) defined on the parent folder of an object. These access rights control the operations a user can perform on the folder and any objects under that folder.

role

An instance of a role template that is applied to a set of Users/Groups for a specific security context. Roles are granted to Users/Groups which allows them access to objects with certain permissions. Some examples of roles are: Process Owner, Control Owner, and Tester.

Role template

A security object that you can use to define all aspects of application security for various groups and users within a business unit. It contains access control definitions on folder structures for object types and application permissions. Role templates generally reflect the usual or expected function that a user or group plays within an organization. Some examples of Role templates that can be defined are Process Owner, Control Owner, and Tester. The template can then be applied to different Users/Groups for a specific security context.

security context point

A point defined in the OpenPages security model that you can use to assign roles to users and groups for controlling access and application permissions to objects under that security point.

security domain group

A group that is automatically created by the system when a business entity or subentity is created. Business entity security domain groups are located under the top level (root) **Security Domains** folder in the  > **Users and Security** > **Domains & Groups** task.

Index

Numerics

3DES [99](#), [103](#)

A

ability to use a template [287](#)

acceptable use link
 login screen [571](#)
 menu item [574](#)

Access Control Lists

 Using inheritance with [1088](#)

access control on Role groups
 settings [636](#)

access controls
 field level [133](#)
 record level [128](#)
 security rules [128](#), [133](#)

access logging [825](#)

accessibility for disabled [600](#)

ACL

 Creating a new [1089](#)
 Deleting an existing [1090](#)
 Editing an existing [1089](#)
 permission values [112](#)
 permissions [111](#)

active reporting period

 about [577](#)
 finalizing [578](#)
 limitations [577](#)
 reapplying [582](#)
 see also Reporting period [581](#)

activity views

 best practices [1110](#)

add

 date dimension type [968](#)
 keys to the Custom folder [576](#)
 report [171](#)
 role template in the Standard UI [118](#)
 role template in the Task Focused UI [114](#)
 tabs to Home page [311](#)

Add New wizard

 availability of object types [286](#)
 configuring [284](#)

Add New Wizard

 disable [600](#)

adding

 dependent fields in SUI [280](#)
 dependent fields in TFUI [279](#)
 dependent pick lists in SUI [290](#)
 dependent pick lists in TFUI [289](#)
 enumerated string values [232](#)
 field groups [206](#), [223](#)
 fields [207](#), [223](#)
 file types [263](#)
 object type dimensions [972](#)
 object type for a custom form [265](#)

adding a custom field for search results [659](#)

adding certificate snap-in
 Microsoft Internet Information Services [787](#)

adding TLS binding
 Microsoft Internet Information Services [789](#)

administering global search [649](#)

Administration menu

 acceptable use [574](#)
 privacy statement [574](#)

administration menus [607](#)

administrator

 Super Administrator [75](#)
 types of permissions [76](#)
 user-provisioning permissions [77](#)

administrator permissions

 assigning [80](#)
 modifying [80](#)
 revoking [80](#)

AES [99](#), [103](#)

alert notification behavior [648](#)

allowed browsers [603](#)

Apache configuration file

 editing [793](#)

Apache load balancer server

 certificate authority approval [794](#)
 editing Apache configuration file [795](#)
 generating a key pair and request [794](#)
 importing the root certificate [795](#)
 TLS configuration [794](#)

Apache web server

 importing the root certificate [790](#)
 importing the server certificate [791](#)

Apache Web Server

 generating a key pair and request [789](#)
 TLS configuration [789](#)

API settings

 enable custom REST service setting [638](#)

application permissions

 Browse Files [96](#)
 Change History [95](#)
 CommandCenter Studios [95](#)
 defining [90](#)
 Folders [96](#)
 Issues [96](#)
 non-SOX [97](#)
 Project Management [96](#)
 setting on a group [90](#)
 View Locks [97](#)

application readiness [843](#)

application server

 default port [763](#)
 Java and process management changes [821](#)
 JDBC connection pools [821](#)
 session management [821](#)
 threadpool sizing [821](#)

application servers

 starting Windows service [841](#)

- application servers (*continued*)
 - stopping Windows service [843](#)
- application text
 - about [564](#)
 - folder categories [564](#)
 - modifying in the Standard UI [567](#)
 - modifying in the Task Focused UI [566](#)
 - report keys [179](#)
- application, starting [841](#)
- applications folder settings [599](#)
- approval app
 - certification questions [999](#)
 - configuring the JSON file [995](#)
 - customizing the JSON file [1001](#)
- Asian characters [559](#)
- assigning
 - permissions [80](#)
 - roles to user or group [119](#)
- associating
 - group [89](#)
 - profiles to users and groups [302](#)
- association
 - relationship [258](#), [259](#)
- association heuristic (reassigning primary parents) [639](#)
- asynchronous background jobs [681](#), [682](#), [715](#), [716](#)
- audit
 - Audit Change Report [168](#)
 - audit change values [169](#)
 - event [168](#)
 - filter settings [648](#)
 - Primary association [168](#)
- audit configuration changes [770](#)
- audit management events settings [648](#)
- Audit Report [771](#)
- aurora log file
 - backing up [829](#), [832](#)
 - maximum size [829](#), [832](#)
- aurora.properties file
 - preparing passwords [101](#)
- auroralogging.properties [829](#), [832](#)
- automatic restart [841](#)

B

- back icon [599](#)
- background jobs [681](#), [682](#), [715](#), [716](#)
- background processes [681](#), [715](#)
- backing up
 - aurora log file [829](#), [832](#)
- backup utility
 - OpenPages application server [682](#), [718](#)
 - overview [682](#), [718](#)
- Backup utility
 - refreshing a test environment [696](#)
- Backup Utility
 - .zip file [684](#), [688](#), [722](#), [727](#)
 - about [679](#), [690](#), [713](#)
 - CommandCenter [687](#)
 - custom files [50](#), [683](#), [719](#)
 - large files [684](#), [688](#), [722](#), [727](#)
 - log files [685](#), [688](#), [722](#), [727](#)
 - manifest file [50](#), [683](#), [719](#)
 - OPBackup file formats [685](#), [722](#)
 - OPCCBackup file formats [688](#), [727](#)

- Backup Utility (*continued*)
 - OpenPages CommandCenter [724](#)
 - password encryption [717](#)
 - refreshing a test environment [694](#), [736](#)
 - running [719](#)
 - running background jobs [681](#), [715](#)
 - running live backups [684](#), [721](#)
 - running OPCCBackup [687](#), [695](#), [726](#)
 - storage [685](#), [722](#)
- bandwidth, improve [817](#)
- batch processing [915](#)
- best practices
 - Chrome [1109](#)
 - configuring Cognos reports [1112](#)
 - deleting unused object types [1111](#)
 - dependent picklists [1110](#)
 - display reporting fragments on demand [1112](#)
 - field dependencies [1110](#)
 - field groups [1109](#)
 - field names [1109](#)
 - limit complexity of security rules [1110](#)
 - limit number of objects [1109](#)
 - limit number of portlets on home page [1110](#)
 - limit number of security rules [1110](#)
 - limit number of SOXBusEntity objects in system [1111](#)
 - limiting associations in the overview [1109](#)
 - minimizing starting groups [1113](#)
 - OPX functionality [1109](#)
 - security rules [143](#)
 - shared field groups [1111](#)
 - using activity views [1110](#)
- Boolean
 - data type [203](#)
- browser
 - best practices [839](#)
 - locale settings [839](#)
 - security [838](#)
 - setting time out [836](#)
- browser back and forward icons [599](#)
- browser configuration
 - Certificate Authority certificates [785](#)
- browsers
 - troubleshooting
 - known problems and solutions [836](#)
- bucket heading [567](#)
- bulk move
 - Allow Hierarchical Moves setting [633](#)
- business entity selector fields
 - adding to views in the Task Focused UI [412](#)

C

- CAF setting [838](#)
- cardinality settings, modifying [262](#)
- cascading signature settings [621](#)
- certificate authority approval
 - Apache load balancer server [794](#)
 - IBM HTTP [792](#), [797](#)
 - web server [788](#), [790](#)
- Certificate Authority certificates [785](#)
- certificate renewal [804](#)
- certificate renewal on WebSphere [806](#)
- Certificate Signing Request file [783](#)
- certificates

- certificates (*continued*)
 - iKeyman tool [792, 797, 798](#)
 - importing [783](#)
 - importing into Java [785](#)
- certification
 - approval app [999](#)
- changing IP address for Oracle server [777](#)
- check-out [602](#)
- child objects
 - access controls [128](#)
 - more than the maximum number of associations [257](#)
 - security rules [136](#)
- Codes
 - Locale [559](#)
- cognitive services
 - configuring [1023, 1026, 1030, 1031](#)
 - configuring in Task Focused UI [1028](#)
 - configuring in the Standard UI [1029](#)
- Cognos
 - services [849](#)
- Cognos Application Firewall [838](#)
- Cognos dashboards and stories
 - creating instances of [177](#)
- Cognos TLS certificate renewal on Apache [805](#)
- Cognos TLS certificate renewal on IIS [804](#)
- colors
 - in the Task Focused UI [409](#)
- command line
 - Security Directory Integrator [988](#)
- CommandCenter
 - Backup Utility [687](#)
 - restore utility [728](#)
- common folder settings [635](#)
- Compare Environments tool
 - Export Max Rows setting [638](#)
 - Max Memory setting [638](#)
- compressing files for upload [613](#)
- compression
 - see HTTP compression [817](#)
- computed field definitions
 - exporting [906](#)
- computed fields
 - creating [225](#)
 - creating with multiple namespaces [229](#)
 - defining [227](#)
 - expression [226](#)
 - importing [226](#)
 - model an equation [226](#)
 - nesting [229](#)
 - report specification [226](#)
- configuration changes
 - migrating [865](#)
- configuration files
 - Apache load balancer server [795](#)
- Configuration Settings
 - modifying in the Standard UI [598](#)
 - modifying in the Task Focused UI [597](#)
- configure
 - embedded reports [317](#)
 - My Reports [317](#)
 - password requirements [99](#)
 - reports on a Home page [316](#)
- configuring
 - password policies [99](#)
- configuring (*continued*)
 - security provider [101](#)
- Configuring cognitive services [1021](#)
- configuring email notifications [982](#)
- configuring global search [655](#)
- configuring global search properties [671](#)
- configuring global search settings [660](#)
- Configuring GRC Workflow [495](#)
- configuring Loss Event Entry [1010](#)
- Configuring loss event entry [1003](#)
- Configuring loss event entry, how to configure the confirmation email [1009](#)
- Configuring loss event entry, how to dates are validated [1006](#)
- Configuring loss event entry, how to launch [1006](#)
- Configuring loss event entry, how to plan [1003](#)
- Configuring loss event entry, how users are handled [1005](#)
- Configuring loss event entry, where loss events get created [1005](#)
- Configuring questionnaire assessments [991](#)
- Configuring the reporting framework [951](#)
- Configuring the reporting framework, how to plan [956](#)
- Configuring the Scheduler [551](#)
- Configuring the Task Focused UI [363](#)
- Configuring Watson Assistant [1013](#)
- Connection Refused error message
 - troubleshooting [989](#)
- connector currency values
 - specifying [986](#)
- connector date values
 - specifying [986](#)
- connectors [986](#)
- context panes [327](#)
- controller conditions
 - copying [282](#)
- cookieSecure [786](#)
- Copy Access From Inactive setting [603](#)
- copy operation settings [614](#)
- Copy User Info Attributes setting [604](#)
- Copy User Info Choice setting [604](#)
- copy views to profile [330](#)
- copying access from one user to another [87](#)
- creating
 - computed fields [225](#)
 - long string index [747](#)
 - long string index in Db2 [703](#)
 - organizational group [89](#)
 - scheduled jobs to synchronize long string index [705, 749](#)
 - user accounts [84](#)
- creating a profile in the Standard UI [299](#)
- creating a profile in the Task Focused UI [298](#)
- creating public filters
 - object types [249, 252–256, 264–267, 271, 273, 308, 322, 1111](#)
- creation views
 - defining [343](#)
- Creation Views
 - adding a card layout [414](#)
 - adding a classifier field that makes object association suggestions [430](#)
 - adding a classifier field that makes taxonomy suggestions [410](#)
 - adding a grid layout [425](#)

Creation Views *(continued)*

- adding actions to relationship fields [434](#)
- applying colors to enumerated fields [407](#)
- applying colors to value ranges [408](#)
- arranging fields in columns [400](#)
- defining a Get Watson Classifier action [438](#)
- defining a Recursive Copy action [436](#)
- defining an Add New action [435](#)
- defining an Associate action [434](#)
- defining an Associate Primary Parent action [435](#)
- defining dynamic filters on relationship fields [438](#)
- defining in the Task Focused UI [391](#)
- designing in the Task Focused UI [377](#)
- displaying a number field as a progress bar [410](#)
- displaying a URL field as a button or link [410](#)
- planning in the Task Focused UI [376](#)
- using in the Task Focused UI [377](#)
- cross-context sharing [641](#)
- cross-site scripting
 - filter setting [645](#)
 - Safe Tags setting [646](#)
- CSR file
 - generating [783](#)
- csv file
 - formatting [214](#)
 - uploading in Standard UI [237](#)
 - uploading in Task Focused UI [215](#)
- cultures [560](#)
- currency
 - data type [203](#)
- currency display type
 - editing [236](#)
 - viewing [236](#)
- currency exchange rates
 - adding [214](#)
 - currency exchange rates
 - disabling in Task Focused UI [215](#)
 - disabling in Standard UI [237](#)
 - editing [213](#)
 - editing in Standard UI [237](#)
 - editing in Task Focused UI [215](#)
 - enabling in Standard UI [237](#)
- currency field definitions
 - exporting [905](#)
 - importing [904](#)
- currency field values
 - editing [236](#)
- Custom folder
 - adding new keys [576](#)
 - using [576](#)
- custom forms
 - adding [265](#)
 - associating to an object [266](#), [267](#)
 - setting up [265](#)
- custom jobs
 - defining in the Scheduler [553](#)
 - implementing a Java class [556](#)
 - managing in the Scheduler [551](#)
 - running in the Scheduler [551](#)
- custom settings
 - create [634](#)
 - delete [634](#)
- customizing global search after initial enablement [657](#)
- customizing global search on initial enablement [656](#)

cyclic relationships [258](#)

D

- dashboard and story templates
 - modifying existing [178](#)
- Dashboard tab
 - troubleshooting JSON export [1106](#)
- Dashboards
 - configuring in the Task Focused UI [367](#)
- data load template [927](#)
- data source [779](#)
- data types
- data types
 - Boolean [203](#)
 - currency [203](#)
 - date [203](#)
 - decimal [203](#)
 - enumerated string [203](#)
 - fragment [203](#)
 - integer [203](#)
 - long string [203](#)
 - security rules [137](#)
 - selecting [203](#)
 - simple string [203](#)
 - single file [203](#)
- database
 - about online backups [729](#)
 - changing references [778](#)
 - crash recovery [736](#)
 - Db2 back up and restore [690](#)
 - disable online backup [736](#)
 - online backup [728](#)
 - Oracle 10g [777](#)
 - RMAN [728](#)
- database passwords
 - updating [774](#)
- database references, change [778](#)
- database server
 - default port [763](#)
- datapump [713](#)
- date
 - data type [203](#)
- date data types [137](#)
- date type dimension
 - add [968](#)
 - delete [970](#)
 - disable or enable [970](#)
 - modify [970](#)
- date type dimensions
 - using [968](#)
- Db2
 - back up and restore database [690](#)
- Db2 database
 - tuning [822](#)
- Db2 Text Search
 - enabling for long string filtering [702](#)
- decimal
 - data type [203](#)
- decrypting
 - OpenPages repository [153](#)
- Default Allowed Profiles setting [604](#)
- default object in parent picker [288](#)
- Default User Change Password setting [604](#)
- Default User Password Expiration setting [605](#)

- default value
 - enumerated string values [233](#)
- defining
 - application permissions [90](#)
- Definition worksheet
 - parameters [935](#)
 - unhide [935](#)
- delegate activities
 - administrator [75–77](#)
- deleting
 - dependent fields [278, 282, 284](#)
 - dependent picklists [293](#)
 - filters [267, 268, 271, 273, 275–277, 702, 703, 705, 707, 746–751](#)
 - object field definitions [225](#)
 - profiles [301](#)
 - rules [143](#)
- deletion interval for reporting period [602](#)
- dependent field
 - adding in SUI [280](#)
 - adding in TFUI [279](#)
 - modifying controllers [282](#)
- dependent fields
 - copying controller fields [282](#)
 - deleting [143, 225, 277, 284, 293, 301](#)
- dependent picklists
 - adding in SUI [290](#)
 - adding in TFUI [289](#)
 - as dimensions [967](#)
 - best practices [1110](#)
 - configure [288](#)
 - deleting [293](#)
 - enabling or disabling [292](#)
 - modifying [292](#)
- deployments [865](#)
- development deployment [865](#)
- dimensions
 - about [953](#)
 - date [968](#)
 - enumerated strings [967](#)
 - picklists [967](#)
- disabling
 - field level encryption keystore [153](#)
 - profiles [297–301](#)
- disabling associations between
 - object types [249, 252–256, 264–267, 271, 273, 308, 322, 1111](#)
- disassociating
 - group [89](#)
 - profiles from users [304](#)
- display columns in selectors [606](#)
- display of tabs with no fields [286](#)
- display order
 - of object types [308](#)
- display types
 - enumerated strings [361](#)
 - long strings [358](#)
 - reporting fragments [348](#)
 - simple strings [349](#)
- domains [73](#)
- dropping
 - long string index [707, 750](#)
- dynamic fields [278](#)
- dynamic tables

dynamic tables (*continued*)

- about [314](#)
- configure [314](#)
- edit [316](#)

E

- e-mail
 - configure OPBackup notification [679, 714](#)
- editing
 - profiles [297–301](#)
- editing properties
 - object types [249, 252–256, 264–267, 271, 273, 308, 322, 1111](#)
- editing properties (Task Focused UI)
 - object types [249, 252–256, 264–267, 271, 273, 308, 322, 1111](#)
- email
 - configure Notification Manager [1075](#)
- email notifications
 - configuring [982](#)
 - customizing for GRC Calculations [492](#)
 - customizing for GRC Workflow [548](#)
- embedded reports
 - configure [317](#)
 - performance considerations [318](#)
 - working with [317](#)
- enable associations of child objects [623](#)
- enable custom REST service setting [638](#)
- enable icons on locked objects [623](#)
- enabling
 - currency exchange [903](#)
 - field level encryption keystore [152](#)
 - OpenPages repository [152](#)
 - profiles [297–301](#)
- enabling a view [327](#)
- enabling and disabling
 - field dependency behavior [283](#)
- enabling associations between
 - object types [249, 252–256, 264–267, 271, 273, 308, 322, 1111](#)
- enabling file attachment search [654](#)
- enabling file types for search [654](#)
- enabling global search [653](#)
- enabling or disabling
 - dependent picklists [288–290, 292, 293, 967, 1110](#)
- enabling or disabling object types or fields for global search [655](#)
- encryption
 - field level [152](#)
 - password [148](#)
- encryption algorithm
 - change AES key [104](#)
 - legacy systems [103](#)
 - UPEA tool [99](#)
- encryption key
 - algorithm [146](#)
 - changing AES [104](#)
- encryption keystore
 - editing [153](#)
- Entity Move/Rename Utility
 - about [708, 758](#)
 - input file [710, 759](#)
 - run as a scheduled task [712, 762](#)

- Entity Move/Rename Utility (*continued*)
 - run interactively [711](#)
- enumerated string
 - data type [203](#)
- enumerated string values
 - adding [232](#)
 - as dimensions [967](#)
 - changing the order of [233](#)
 - default value [233](#)
 - deleting [235](#)
 - hiding [234](#)
 - unhiding [234](#)
- environment files
 - password encryption [717](#)
- environment migration
 - best practices [872](#)
 - dependent items migrated [868](#)
 - exporting items [873](#), [874](#)
 - importing items [875](#)
 - items migrated [866](#)
 - items not migrated [869](#)
 - process of [872](#)
 - settings [612](#), [865](#)
 - validating the import [875](#)
- environments
 - comparing [853](#)
- equation editor
 - about [637](#)
- equations
 - modeling [226](#)
- Excel worksheet. See FastMap. [920](#)
- excluding
 - object types from an overview page [334](#)
- excluding fields
 - object type [255](#), [304–306](#), [333](#)
- excluding from a profile
 - object type [255](#), [304–306](#), [333](#)
- excluding object types
 - profile [302](#), [304](#), [305](#), [322](#), [330](#)
- excluding settings from migrating [909](#)
- Export Max Rows [638](#), [855](#)
- exported XML files
 - comparing [853](#)
- exporting
 - computed field definitions [906](#)
 - configuration data [865](#)
 - currency field definitions [905](#)
 - data [881](#)
 - workflow definitions [452](#), [548](#)
- exporting configuration changes [911](#)
- exporting data [911](#)
- exporting metadata changes
 - ObjectManager [881](#), [885](#), [909](#), [1085](#)
- expressions for GRC Calculations
 - functions for currency values [485](#)
 - functions for dates [483](#)
 - functions for lists and numerical values [481](#)
 - functions for string values [479](#)
 - If/then/endif statements [486](#)
 - syntax rules [471](#)
 - testing and debugging [491](#)
 - tutorial [473](#)
 - using system variables [478](#)
- EXTEND rule [122](#)

- external system, import data [945](#)

F

- facts
 - about [953](#), [974](#)
 - disabling [966](#)
 - enabling [966](#)
- facts and dimensions
 - process for configuring [966](#)
- facts and dimensions, configuring [966](#)
- FAQs
 - global search [675](#)
- FastMap
 - access in Standard UI [919](#)
 - access in Task Focused UI [918](#)
 - define the path of an object [928](#)
 - Definition worksheet [934](#)
 - errors and warnings [920](#)
 - export data into template [927](#)
 - export template [935](#), [936](#)
 - Filtered List View page export settings [628](#)
 - import jobs [919](#)
 - import process [916](#)
 - import status [925](#), [926](#)
 - import status window in Standard UI [926](#)
 - JSP [935](#)
 - locale [917](#)
 - optimize performance [947](#), [948](#)
 - overview [915](#)
 - parameters [935](#), [937](#)
 - securing import templates [948](#)
 - template [916](#)
 - user profile [917](#)
 - validation [917](#)
 - validation messages [921](#)
 - worksheet [916](#)
- field dependencies
 - best practices [1110](#)
- field dependency behavior
 - enabling and disabling [283](#)
- field groups
 - adding [206](#), [223](#)
 - adding fields to [207](#), [223](#)
 - best practices [1109](#)
 - best practices for shared [1111](#)
 - deleting [225](#)
 - including in an object type [255](#)
- field guidance [600](#)
- field level encryption
 - disabling the keystore [153](#)
 - enabling the keystore [152](#)
 - key [146](#)
 - keystore [146](#), [147](#)
- field level security
 - redaction
 - field level security [134](#)
 - security
 - field level [135](#)
- field names
 - best practices [1109](#)
- fields
 - decrypting
 - fields [210](#)

- fields (*continued*)
 - encrypting
 - field values [209](#)
 - encrypting values for [209](#)
 - excluded [295](#)
 - including in an object type [306](#)
 - long string
 - encrypting [209](#)
 - simple string
 - encrypting [209](#)
 - system workflow fields [502](#)
- fields from an object type
 - excluding [305](#), [306](#), [334](#)
- file
 - check-out [602](#)
 - checked in [602](#)
- file attachment search
 - enabling [654](#)
 - enabling file types [654](#)
- file type information
 - configuring [263](#)
- file types
 - adding [263](#)
 - associating with object types [264](#)
 - removing [264](#)
- file upload, setting [613](#)
- filtered list view
 - about [324](#)
 - grid view pages
 - configuring [324](#)
- Filtered List view
 - add object fields [332](#), [344](#)
 - disabling [328](#)
 - remove object fields [333](#)
- Filtered List View
 - displaying initial results [628](#)
 - FastMap export [628](#)
 - remove object fields [345](#)
- filtered list view settings [628](#)
- filters
 - adding to object types [273](#)
 - adding to object types (Task Focused UI) [271](#)
 - associating views [275](#)
 - considerations before you begin [268](#)
 - copying [276](#)
 - creating Db2 long string index [703](#)
 - creating long string index [747](#)
 - creating scheduled jobs to synchronize long string indexes [705](#), [749](#)
 - currently logged on user [276](#)
 - deleting [143](#), [225](#), [277](#), [284](#), [293](#), [301](#)
 - dropping long string indexes [707](#), [750](#)
 - enabling DB2 Text Search for long strings [702](#)
 - enabling Oracle Text for long strings [748](#)
 - modifying [277](#)
 - stop words for long string indexes [751](#)
 - utilities for long strings [702](#), [746](#)
- Fix Central [1099](#)
- folder view
 - about [324](#)
- Folder view
 - disabling [328](#)
- folder view pages
 - configuring [324](#)

- fragment
 - data type [203](#)
- framework generator port [768](#)
- Framework Model Generator
 - starting and stopping on Windows [850](#)
- Framework Model Generator service
 - starting and stopping on Linux [850](#)

G

- generating a CSR
 - iKeyman tool [792](#), [796](#)
- generating a key pair and request
 - Apache Web Server [789](#)
- generating a keystore and key pair
 - IBM HTTP server [791](#), [796](#)
- global search
 - add a custom field [659](#)
 - administering [649](#)
 - configuring [655](#)
 - customizing after initial enablement [657](#)
 - customizing on initial enablement [656](#)
 - enabling [653](#)
 - enabling or disabling object types or fields [655](#)
 - OPBackup and OPRestore [653](#)
 - properties [671](#)
 - settings [660](#)
 - starting services [844](#)
 - stopping services [845](#)
 - unhiding settings [660](#)
- global search FAQs [675](#)
- global search properties
 - error handling parameters for the indexer [671](#)
 - maximum file attachment text for indexing [674](#)
 - maximum heap size [672](#)
 - maximum opsearchtool.jar heap size during indexing [672](#)
 - maximum Solr heap size [672](#)
 - maximum text extraction heap size during indexing [673](#)
 - root path location for file attachment search [674](#)
 - setting the text extractor timeout limit [673](#)
- globalization [560](#)
- GRC Calculations
 - building expressions [471](#)
 - calculate on object save [457](#)
 - calculation definitions [458](#), [466](#)
 - cascade effect [463](#)
 - configuring [457](#)
 - customizing email notifications [492](#)
 - defining [467](#)
 - designing [463](#)
 - FAQs [461](#)
 - functions for currency values [485](#)
 - functions for dates [483](#)
 - functions for lists and numerical values [481](#)
 - functions for string values [479](#)
 - how to delete a calculation [466](#)
 - how to disable a calculation [466](#)
 - how to publish a calculation [466](#)
 - how to save a calculation [466](#)
 - If/then/endif statements [486](#)
 - permissions [457](#)
 - running as administrator [490](#)
 - syntax rules for expressions [471](#)

- GRC Calculations (*continued*)
 - system variables [478](#)
 - testing and debugging [491](#)
 - tutorial for writing expressions [473](#)
 - use cases [464](#)
- GRC Workflow
 - assignees [498](#)
 - configuring [495](#)
 - customizing email notifications [548](#)
 - defining a standard stage [519](#)
 - defining a workflow [513](#)
 - defining an end stage [523](#)
 - defining applicability for a workflow [514](#)
 - defining assignees for a stage [519](#)
 - defining autostart or manual start for a workflow [514](#)
 - defining criticality for a workflow [514](#)
 - defining overall due date for a workflow [514](#)
 - defining oversight users for a workflow [514](#)
 - defining stage due dates [519](#)
 - defining stage properties [519](#), [523](#)
 - defining subscribers for a stage [519](#)
 - defining task view overrides for a stage [519](#)
 - defining workflow properties [514](#)
 - designing a workflow [505](#)
 - due dates [505](#)
 - enabling and disabling a workflow [514](#)
 - exporting and importing workflow definitions [548](#)
 - fundamental concepts [496](#)
 - GRC workflow designer [508](#)
 - how to start a workflow [499](#)
 - how users interact with workflows [499](#)
 - implementing a Java class [1117](#)
 - inserting fields, URLs, and application text [503](#)
 - inserting variables [503](#)
 - managing workflow instances [547](#)
 - oversight users [498](#)
 - participants [498](#)
 - permissions [495](#)
 - running reports that include workflow information [550](#)
 - stage due dates [505](#)
 - starting workflow instances in bulk [546](#)
 - subscribers [498](#)
 - system workflow fields [502](#)
 - workflow definitions [496](#)
 - workflow due date [505](#)
 - workflow instances [496](#)
- grid view
 - defining [335](#)
- grid views
 - disabling [328](#)
- Grid Views
 - applying colors to enumerated fields [407](#)
 - applying colors to value ranges [408](#)
 - defining default filters for Grid Views [406](#)
 - defining in the Task Focused UI [389](#)
 - designing in the Task Focused UI [374](#)
 - displaying a number field as a progress bar [410](#)
 - planning in the Task Focused UI [373](#)
 - using in the Task Focused UI [373](#)
- Group Selector [358](#)
- groups
 - associating [89](#)
 - associating profiles [302](#)
 - creating [89](#)

- groups (*continued*)
 - disassociating [89](#)
- Groups
 - Nested [1093](#)
 - Using to limit user activities [1091](#)
- gzip format [685](#), [688](#), [722](#), [727](#)

H

- helpers
 - timesheet approval [993](#)
 - timesheet entry [993](#)
- hidden settings [602](#)
- home page
 - best practices for limiting portlets [1110](#)
 - Cognos reports [1112](#)
- Home page
 - configure reports [316](#)
 - configure the Dashboard tab [319](#)
 - configure the My Work tab [313](#)
 - configuring tabs [311](#)
 - considerations [310](#)
 - creating content on the Dashboard tab [320](#)
 - display order of tabs [312](#)
 - dynamic tables [314](#)
 - editing content on the Dashboard tab [321](#)
 - exporting configuration of the Dashboard tab [322](#)
 - hide or unhide tabs [312](#)
 - in the Task Focused UI [367](#)
 - JSON download [322](#)
 - layout of tabs [310](#)
 - My Work
 - Dashboard [309](#)
 - overview [309](#)
 - pre-defined tables [314](#)
 - Tab Configuration table [311](#)
 - tabs [309](#)
- host name, database server [778](#)
- host setting [640](#)
- HTTP
 - security [645](#)
- HTTP compression
 - about [817](#)
 - disabling [817](#)
- http_access.log [825](#)
- httpd.conf file
 - editing [793](#)
- httpSession [786](#)
- hyperlinking
 - to object instances, views, filters [1113](#)

I

- IBM Cognos service
 - starting and stopping [849](#)
 - starting and stopping on Linux [850](#)
 - starting and stopping on Windows [849](#)
- IBM HTTP
 - certificate authority approval [792](#), [797](#)
- IBM HTTP server
 - generating a keystore and key pair [791](#), [796](#)
 - TLS configuration [796](#)
- IBM OpenPages

- IBM OpenPages (*continued*)
 - restore [679](#)
- IBM OpenPages application and database
 - backup [679](#), [713](#)
 - Db2 back up and restore [690](#)
 - restore [679](#), [713](#)
- IBM OpenPages CommandCenter
 - backup [679](#)
 - Db2 back up and restore [690](#)
- IBM OpenPages SDI Connector for UCF Common Controls Hub [986](#)
- IIS [818](#)
- iKeyman tool
 - generating a CSR [792](#), [796](#)
 - importing certificates [792](#), [797](#), [798](#)
- import data
 - external system [945](#)
 - see also FastMap [915](#)
- importing
 - configuration data [865](#)
 - currency field definitions [904](#)
 - data [881](#)
 - workflow definitions [452](#), [548](#)
- importing changes [913](#)
- importing configurations [913](#)
- importing root certificate
 - Microsoft Internet Information Services [788](#)
- importing the server certificate
 - Apache web server [791](#)
- indexes
 - adding [642](#)
 - example [643](#)
- inline guidance
 - adding to views in the Task Focused UI [400](#)
- installation
 - default ports [763](#)
- instance name, database [778](#)
- integer
 - data type [203](#)
- interactive reports [554](#)
- interactive task
 - Entity Move/Rename Utility [711](#)
- IP address
 - static [777](#)

J

- Java
 - importing certificates [785](#)
- Java and process management changes
 - application server [821](#)
- Java classes
 - implementing for custom jobs [556](#)
 - implementing for GRC Workflow [1117](#)
- java.security file [101](#)
- JDBC connection pools
 - application server [821](#)
- JDBC data source [779](#)
- JSON export
 - troubleshooting [1106](#)
- JSON file
 - configuring for approval app [995](#)
 - customizing for approval app [1001](#)
- JSON in the Task Focused UI

- JSON in the Task Focused UI (*continued*)
 - applying colors to value ranges [408](#)
 - arranging fields in columns [400](#), [407](#)
 - inline guidance [400](#)
 - Task View header [404](#)
 - tips for editing [398](#)
- JSP files [252](#)
- JSP report jobs
 - defining in the Scheduler [554](#)

K

- key pair and request
 - Apache load balancer server [794](#)
 - Microsoft Internet Information Services [787](#)
- keys [576](#)
- keystore
 - Db2 [773](#)
 - WebSphere Liberty [772](#)
- keywords
 - security rules
 - field level [137](#)
 - record level [137](#)

L

- languages [560](#)
- LDAP
 - authentication module, configuring [155](#)
 - configuring for user accounts [81](#), [82](#)
 - mixed-mode authentication [157](#)
 - user authentication [154](#)
- legacy move behavior [640](#)
- Linux load balancer server
 - TLS configuration [791](#)
- list view pages [327](#)
- live backup [684](#), [721](#)
- loading
 - data [881](#)
- locale browser settings [839](#)
- Locale codes [559](#)
- localizing
 - system fields [564](#)
- lock and signature settings [619](#)
- lock menu for display settings [621](#)
- lock menu settings [622](#)
- locked
 - parent object [622](#)
- locked objects
 - enabling associated object icons [623](#)
- locking a user account [644](#)
- locks
 - enabling and disabling [620](#)
 - objects [621](#)
- log files
 - access logging [825](#)
 - OPBackup [685](#), [722](#)
 - OPCCBackup [688](#), [727](#)
 - OPCCRestore [690](#), [728](#)
 - OPRestore [687](#), [724](#)
- login screen
 - messages [571](#)
- long string

- long string (*continued*)
 - data type [203](#)
- long string fields
 - running string concatenation [752](#)
 - string concatenation SQL file [754](#)
 - String Concatenation Utility [752](#)
- long string indexes
 - creating [747](#)
 - creating in Db2 [703](#)
 - creating scheduled jobs to synchronize [705](#), [749](#)
 - dropping [707](#), [750](#)
 - enabling Db2 Text Search [702](#)
 - enabling Oracle Text [748](#)
 - stop words [751](#)
 - utilities [702](#), [746](#)
- loops [258](#)
- LTPA token [786](#)

M

- mail server address
 - setting [612](#)
- managing for object types
 - filters [267](#), [268](#), [271](#), [273](#), [275–277](#), [702](#), [703](#), [705](#), [707](#), [746–751](#)
- managing object types [249](#)
- map to date fields [969](#)
- Max File Upload Size [855](#)
- Max Memory [638](#), [855](#)
- menus
 - hiding menu items [608](#)
 - modifying submenu items [607](#)
 - modifying the order of [607](#)
- messaging information [825](#)
- Microsoft Internet Information Services
 - adding certificate snap-in [787](#)
 - adding TLS binding [789](#)
 - importing root certificate [788](#)
 - key pair and request [787](#)
- migrating
 - data [881](#)
- migrating configuration changes [907](#)
- migrating environments, *See* environment migration
- migration
 - configuration changes [865](#)
- mode setting [620](#)
- models, adding using the template model [961](#)
- models, reporting framework [951](#)
- modify
 - role template [115](#)
- modify settings in the Standard UI [598](#)
- modify settings in the Task Focused UI [597](#)
- modify text displayed in the Standard UI [567](#)
- modify text displayed in the Task Focused UI [566](#)
- modifying
 - controllers for dependent field [282](#)
 - stop words for long string indexes [751](#)
 - user accounts [86](#)
- move entities
 - Entity Move/Rename Utility [708](#), [758](#)
 - Entity Move/Rename Utility input file [710](#), [759](#)
- multi-deployment environments [907](#)
- Multi-Valued Group Selector [358](#)
- Multi-Valued User Selector [358](#)

- Multi-Valued User/Group Selector [358](#)
- multiple security context points [109](#)

N

- namespace
 - definition [952](#)
 - dimensional [974](#)
 - overview [952](#)
 - relational [974](#)
- namespaces [963](#)
- Namespaces and models, configuring [961](#)
- Natural Language Classifier
 - adding a classifier field that makes object association suggestions [430](#)
 - adding a classifier field that makes taxonomy suggestions [410](#)
- Natural Language Understanding
 - configuring [1025](#)
- navigation bar
 - hide menu items [608](#)
 - modify menu items [607](#)
 - modify menu order [607](#)
- navigational view
 - remove view page [328](#)
- Navigational View
 - configuring [323](#)
- new features in version 7.3.0 [29](#)
- new features in version 7.3.0.1 [28](#)
- new features in version 7.3.0.2 [27](#)
- new features in version 7.4.0
 - administration and serviceability [25](#)
 - platform enhancements [24](#)
- new features in version 8.2.0 [9](#)
- new features in version 8.2.0.1 [6](#)
- new features in version 8.2.0.2 [4](#)
- new features in version 8.2.0.3 [2](#)
- new features in version 8.2.0.4 [1](#)
- New User Default Locale setting [605](#)
- Notification Manager
 - properties [1085](#)
- numeric data types [137](#)

O

- object aspect [168](#)
- object field definitions
 - deleting [225](#)
 - modifying [224](#)
- object fields
 - Business Entity Selector types for simple strings [350](#)
 - display types for enumerated strings [361](#)
 - display types for long string fields [358](#)
 - identifying new [200](#)
 - modifying the phonebook [358](#)
 - on demand display types for long string fields [359](#)
 - rich text area display types for simple strings [349](#)
 - rich text display types for medium long string fields [360](#)
 - Schema Analysis report [202](#)
 - setting a default value for [210](#)
 - setting the display order of [329](#)
 - text and URL display types for simple strings [351](#)
 - text area display types for simple strings [353](#)

- object fields (*continued*)
 - text display types for medium long string fields [360](#)
 - threshold limit [202](#)
 - user and group selector display types for simple strings [353](#)
 - using a rich text display type to configure a URL field [352](#)
- Object fields
 - display types for simple string fields [349](#)
 - Modifying user and group selectors [358](#)
 - read-only [347](#)
- object icons [623](#)
- Object Manager tool [909](#)
- object model diagrams
 - viewing in the solution schema visualization editor [250](#)
- object models
 - viewing in the solution schema visualization editor [250](#)
- object reset
 - performing [592](#)
 - ruleset parameters [592](#)
 - session details [593](#)
 - session log [594](#)
 - starting in the Standard UI [594](#)
 - starting in the Task Focused UI [592](#)
 - status [593](#)
- object resets
 - currency fields [583](#)
 - overview [577](#)
 - preparing data [583](#)
 - system fields [583](#)
- object text [561](#)
- object type
 - including field groups [255](#)
 - including fields [306](#)
 - including in a profile [304](#)
 - including on an overview page [333](#)
- object type definitions
 - accessing [253](#)
- object type dimensions
 - adding [972](#)
- object type dimensions, configuring [972](#)
- object type profiles
 - editing [253](#), [254](#), [300](#)
- object type profiles(Task Focused UI)
 - editing [253](#), [254](#), [300](#)
- object types
 - adding filters [273](#)
 - adding filters (Task Focused UI) [271](#)
 - adding for a custom form [265](#)
 - associating with file types [264](#)
 - deleting [266](#)
 - deleting unused [1111](#)
 - managing [249](#)
 - platform [249](#)
 - rendering JSP files [252](#)
 - setting the display order [308](#)
 - view pages [322](#)
- object types from a profile
 - excluding [305](#), [306](#), [334](#)
- object views
 - customizing [322](#)
- ObjectManager
 - batch loader sample [885](#)
 - batch loader syntax [885](#)
- ObjectManager (*continued*)
 - loader files [881](#)
 - properties [1085](#)
- ObjectManager examples
 - assigning or revoking role assignments [889](#)
 - creating or loading users [891](#)
 - importing file attachments [907](#)
 - moving objects [886](#)
 - renaming objects [887](#)
- ObjectManager tool [881](#)
- objects
 - auto-naming settings [609](#)
 - best practices for limiting in views [1109](#)
 - locking and unlocking [621](#)
 - path expressions [136](#)
 - SOXDocument auto-naming settings [611](#)
- online backup
 - database [728](#)
- op-backup-restore.env file
 - preparing passwords [101](#)
- OP-CUSTOM [103](#)
- OPBackup
 - backup utility [682](#), [718](#)
 - configuring e-mail [680](#), [714](#)
 - configuring gzip [685](#), [688](#), [722](#), [727](#)
 - log files [685](#), [722](#)
 - refreshing a test environment [694](#), [696](#), [736](#)
 - running [719](#)
 - running live backups [684](#), [721](#)
- OPCCBackup
 - about [724](#)
 - configuring e-mail [680](#), [714](#)
 - log files [688](#), [727](#)
 - running [687](#), [695](#), [726](#)
- OPCCRestore
 - log files [690](#), [728](#)
- OpenPages CommandCenter
 - Backup Utility [724](#)
 - restore utility [689](#)
 - running the Backup Utility [687](#), [695](#), [726](#)
- OpenPages repository
 - decrypting [153](#)
 - enabling [152](#)
 - encrypting [152](#)
- OpenPages solutions
 - FCM [xxxii](#)
 - IAM [xxxii](#)
 - ITG [xxxii](#)
 - ORM [xxxii](#)
 - PCM [xxxii](#)
- OpenPages, connectors, and QRadar
 - overview [981](#)
- operators
 - security rules [137](#)
- OPRestore
 - log files [687](#), [724](#)
- OPX functionality
 - best practices [1109](#)
- Oracle
 - backing up databases [720](#)
- Oracle Admin Client [713](#)
- Oracle Data Pump
 - overview [713](#)
- Oracle Enterprise Manager [777](#)

- Oracle Instant Client [713](#)
- Oracle server
 - IP address [777](#)
- Oracle Text
 - enabling for long string filtering [748](#)
- organizational group [89](#)
- Overview
 - best practices for limiting associations [1109](#)
- overview of OpenPages, connectors, and QRadar [981](#)
- overview page
 - adding a view page [327](#)
 - including object types [333](#)
 - removing object types [334](#)
- Overview page
 - about [323](#)
- overview pages
 - hiding an object from [334](#)
 - setting cache capacity [599](#)
- Overview pages
 - configuring [323](#)

P

- page size setting [605](#)
- Palettes
 - in themes [452](#)
- parent object [622](#)
- parent objects
 - access controls [128](#)
 - security rules [136](#)
- password
 - change Oracle Native Driver password [744](#)
 - change Oracle password [775](#)
 - configure [99](#)
 - encryption algorithm [148](#)
 - modify encryption [99](#)
 - policies [99](#)
 - rules [84](#)
- password encryption
 - keystore [147](#)
- passwords
 - changing encryption algorithms [103](#)
 - changing in User table [102](#)
 - preparing for reencryption [101](#)
- path expressions
 - objects [136](#)
- paths
 - children [136](#)
 - parents [136](#)
- permissions
 - application [91](#)
 - assigning [80](#)
 - Browse Files [96](#)
 - Change History [95](#)
 - CommandCenter Studios [95](#)
 - define [90](#)
 - Folders [96](#)
 - GRC Calculations [457](#)
 - GRC Workflow [495](#)
 - Issues [96](#)
 - modifying [80](#)
 - non-SOX [97](#)
 - other application [97](#)
 - Project Management [96](#)
 - permissions (*continued*)
 - revoking [80](#)
 - setting for a group [90](#)
 - Task Focused UI [363](#)
 - View Locks [97](#)
- phonebook [358](#), [567](#)
- phonebook bucket size [605](#)
- picklists
 - dependent [289](#), [290](#)
 - dependent as dimensions [967](#)
 - modifying dependency behavior [292](#)
- Platform folder settings [638](#)
- platform object types [249](#)
- Platform Reporting Framework folder settings [642](#)
- Platform Reporting Schema folder settings [642](#)
- Platform Security folder settings [644](#)
- ports
 - default [763](#)
 - fixed [763](#)
 - virtual hosts [783](#)
- position of tabs on a Home page [312](#)
- postinstallation tasks
 - updating reporting schema [162](#)
- pre-defined tables [314](#)
- Preference Objects
 - and GRC Workflow [505](#)
- primary parent ID
 - specifying [983](#)
- privacy link
 - login screen [571](#)
 - menu item [574](#)
- privacy statement
 - login screen [571](#)
- problem determination
 - exchanging information with IBM Support [1100](#), [1101](#)
- production deployment [865](#)
- profile
 - associating users and groups [302](#)
 - configuring view pages [322](#)
 - copy views [330](#)
 - disassociating users [304](#)
 - including object types [304](#)
 - view pages [322](#)
- profiles
 - creating in the Standard UI [299](#)
 - creating in the Task Focused UI [298](#)
 - default [300](#)
 - deleting [301](#)
 - disabling [153](#), [301](#)
 - editing [253](#), [254](#), [300](#)
 - enabling [152](#), [301](#), [903](#)
 - fallback [300](#)
 - guidelines [297](#)
 - setting default or fallback [300](#)
- properties and parameters
 - aurora.properties [1081](#)
 - server.properties [1083](#)
 - sosa.properties [1084](#)
 - tools.properties [1085](#)
- Properties and parameters [1081](#)
- properties file
 - HTTPS address [798](#)
 - TLS port [798](#)
- properties files

properties files (*continued*)

editing for TLS [786](#)

property bundles

creating [207](#), [223](#)

provisioning users [83](#)

publish reports

application user interface [180](#)

publishing reports

limitations [180](#)

server user interface [177](#)

Q

QRadar integration package

troubleshooting

known problems and solutions [1105](#)

QRadar integration project

using [982](#)

Questionnaire assessments

configuring [991](#)

R

RCM [1039](#), [1067](#), [1071](#)

RCM Theme Deployer [1065](#)

record level security

security

record level [121](#), [126](#)

recursive object types

defining levels [953](#)

rules [954](#)

Redirect Template [171](#)

redirect the security log off link [644](#)

reencryption

password [101](#)

reference

relationship [258](#), [259](#)

reference relationships [258](#)

regenerate

reporting framework [974](#)

reporting schema [159](#)

Reporting schema

accessing in the Standard UI [159](#)

accessing in the Task Focused UI [159](#)

Registry settings, apply to all models [957](#)

relationship

setting [259](#)

Relationship fields in the Task Focused UI

adding a card layout [414](#)

adding a chart diagram [416](#)

adding a count [424](#)

adding a grid layout [425](#)

adding a tree diagram [429](#)

adding actions to [434](#)

defining a Delete action [438](#)

defining a Get Watson Classifier action [438](#)

defining a Recursive Copy action [436](#)

defining an Add New action [435](#)

defining an Associate action [434](#)

defining an Associate Primary Parent action [435](#)

defining dynamic filters on [438](#)

remove all tree locks [623](#)

rename

rename (*continued*)

Allow Hierarchical Moves setting [633](#)

rename entities

Entity Move/Rename Utility [708](#), [758](#)

Entity Move/Rename Utility input file [710](#), [759](#)

Report

add links to My Reports [317](#)

embed on Home page [317](#)

embedded reports performance considerations [318](#)

modify on Home page [318](#)

report fragments

settings [612](#)

reporting fragment fields

configuring display types [348](#)

defining [240](#)

field group for [241](#)

fields requiring parameter information [239](#)

limitations [238](#)

name [241](#)

object ID prompt [242](#)

planning considerations [239](#)

report path [241](#)

reporting period ID prompt [243](#)

size [243](#)

tasks to configure [238](#)

reporting fragments

displaying on demand [1112](#)

reporting framework

accessing [977](#)

generating [974](#)

regenerate [974](#)

update [978](#)

viewing details of [978](#)

Reporting framework

permissions [975](#)

Reporting Framework [952](#)

reporting framework, models [951](#)

reporting framework, understanding [951](#)

reporting period

ACLs [578](#)

application behavior [577](#)

application permissions [579](#)

change history [578](#)

create in Standard UI [580](#)

create in Task Focused UI [579](#)

delete [580](#)

deletion period setting [579](#)

finalize [578](#), [581](#), [583](#)

overview [577](#)

reapplying [582](#)

reporting schema [578](#)

system administration mode [579](#)

Reporting period

active reporting period [581](#)

see also active reporting period [581](#)

reporting schema

adding indexes [642](#)

updating [162](#)

Reporting schema

accessing in the Standard UI [162](#), [163](#)

Administering [159](#)

Creating and recreating in the Task Focused UI [162](#)

Enabling and disabling in the Standard UI [163](#)

Enabling and disabling in the Task Focused UI [162](#)

- Reporting schema (*continued*)
 - index example [643](#)
 - permissions [161](#)
 - Populating past reporting periods [160](#)
 - relation to reporting period [160](#)
 - Viewing in the Task Focused UI [162](#)
 - Viewing operation details of in the Standard UI [164](#)
- reporting server
 - default port [763](#)
 - Tomcat heap size [821](#)
- reporting service
 - tuning [821](#)
- reports
 - Administrative Reports folder [167](#)
 - as Home page tabs [311](#)
 - Audit Reports folder [168](#)
 - creating interactive [181](#)
 - GRC Workflow [550](#)
 - Issue Reports folder [170](#)
 - managing [167](#)
 - running interactive [182](#)
 - Schema Analysis report [202](#)
 - supplied [167](#)
 - top-level [167](#)
 - understanding [172](#)
 - V6 Folder reports [167](#)
 - viewing [171](#)
- Reports
 - Issue [170](#)
 - Security [170](#)
- Reports Access Page Size setting [605](#)
- required fields
 - setting in a profile [307](#)
 - setting in the field definition [209](#)
 - troubleshooting [1106](#)
- resets, *See* object resets
- restore IBM OpenPages database [686](#)
- restore OpenPages database [723](#)
- restore utilities
 - CommandCenter [727](#)
 - OpenPages CommandCenter [689](#)
- Restore Utility
 - about [679](#), [690](#), [713](#)
 - IBM OpenPages [723](#)
 - log files [687](#), [690](#), [724](#), [728](#)
 - running [686](#), [723](#)
- RESTRICT rule [122](#)
- revoking
 - role from user or group [118](#), [120](#)
- RMAN [728](#)
- role
 - assigning to user or group [119](#)
 - revoking from user or group [118](#), [120](#)
- role template
 - create in the Standard UI [118](#)
 - create in the Task Focused UI [114](#)
 - delete [116](#)
 - disabling [115](#)
 - enabling [115](#)
 - modify [115](#)
 - view or modify [113](#)
- role-based security model [105](#)
- root certificate
 - Apache load balancer [795](#)

- root certificate (*continued*)
 - Apache web server [790](#)
- rules, *See* security rules
- rules in the Task Focused UI
 - defining [439](#)
 - editable and readonly rules [440](#)
 - Greater, GreaterEqual, Less, LessEqual, and Equal rules [443](#)
 - MinLength and MaxLength rules [444](#)
 - pattern rules [445](#)
 - required rules [442](#)
- ruleset
 - creating [584](#)
 - exporting XML file [595](#)
 - file, creating [584](#)
 - loading [591](#)
 - overview [577](#)
 - parameters [592](#)
 - sample [585](#)
 - tag library [586–591](#)

S

- SAM
 - enabling and disabling [71](#)
- save as draft [260](#), [261](#)
- scenarios
 - access to issue action items [131](#)
 - all users can view objects, some users can update objects [133](#)
 - exception management [133](#)
 - objects shared across GRC domains [129](#)
 - privacy incidents [133](#)
 - security by function [132](#)
- scheduled task
 - Entity Move/Rename Utility [712](#), [762](#)
- Scheduler
 - configuring [551](#)
 - defining a custom job [553](#)
 - how to delete a custom job [551](#)
 - how to disable a job [551](#)
 - how to run a job [551](#)
 - kinds of jobs [551](#)
 - running JSP reports [554](#)
- scheduling the Security Directory Integrator [988](#)
- schema
 - reporting [162](#)
- SDI [986](#)
- SDI error messages
 - troubleshooting [1105](#)
- search filter
 - using complex logic [274](#)
- section headings [346](#), [347](#)
- security
 - advanced XSS filter setting [645](#)
 - context point [106](#), [107](#)
 - cross-site scripting filter setting [645](#)
 - domain groups [110](#)
 - extending security context [108](#)
 - field level [133](#)
 - model [105](#)
 - model with multiple points [109](#)
 - Safe Tags setting [646](#)
 - triangle relationship [109](#)

security (*continued*)

- White-listed Suspicious Character Combinations setting [647](#)
- Security Directory Integrator
 - command line tips [988](#)
 - scheduling [988](#)
 - techniques [988](#)
- security domains [110](#)
- security model
 - Security Domains folder [110](#)
- security provider
 - configuring [101](#)
- security rules
 - access controls [128](#), [133](#)
 - best practices for [143](#)
 - best practices for limiting [1110](#)
 - child objects [136](#)
 - data types [137](#)
 - deleting [143](#)
 - disabling [142](#)
 - enabling [142](#)
 - exporting [865](#), [881](#)
 - field level [136](#)
 - grammar [139](#)
 - importing [865](#), [881](#)
 - keywords [137](#)
 - operators [137](#)
 - parent objects [136](#)
 - paths [136](#)
 - record level [136](#)
 - reporting periods [577](#)
 - rulesets [577](#), [584](#)
 - scenarios [129](#), [131–133](#)
 - validating [142](#)
- security, browser [838](#)
- SecurityScorecard [1071](#)
- selectors to use for search [607](#)
- self-contained object type
 - about [636](#)
- server properties and parameters [1083](#)
- services
 - Cognos [849](#)
 - starting [841](#)
 - starting and stopping Cognos service [850](#)
 - starting and stopping Framework Model Generator service [850](#)
 - starting and stopping IBM Cognos service [849](#)
 - stopping [843](#)
- session cookies [786](#)
- session management
 - application server [821](#)
- session timeout [836](#)
- set
 - application permissions on a group [90](#)
- setting a default view [329](#)
- setting the relationship type [259](#)
- setting up custom forms [265](#)
- settings
 - access control on Role groups [636](#)
 - access the Settings page [597](#)
 - accessibility [600](#)
 - additional fields in search results [667](#)
 - administration menus [607](#)
 - alert notification behavior [648](#)

settings (*continued*)

- allow compression [667](#)
- Allow Hierarchical Moves [633](#)
- allow URL redirects [668](#)
- allow users to personalize my work home page [626](#)
- allowed browsers [603](#)
- Apache Solr password [670](#)
- Apache Solr user ID [670](#)
- applications folder [599](#)
- association heuristic (reassigning primary parents) [639](#)
- audit management events [648](#)
- auto-naming objects [609](#)
- browser cache [599](#)
- cache capacity [599](#)
- cascading signatures [621](#)
- child and parent [622](#)
- common folder [635](#)
- Copy Access From Inactive [603](#)
- copy operations [614](#)
- Copy User Info Attributes [604](#)
- Copy User Info Choice [604](#)
- copying folders [634](#)
- create custom [634](#)
- cross-context sharing [641](#)
- cross-site scripting filter [645](#)
- date field display format [616](#)
- Default Allowed Profiles [604](#)
- default number of search results to return per page [670](#)
- Default User Change Password [604](#)
- Default User Password Expiration [605](#)
- delete custom [634](#)
- deletion interval for reporting period [602](#)
- disable Add New wizard [600](#)
- display columns for selectors [606](#)
- enable associations of child objects [623](#)
- enable create and delete custom settings [633](#)
- Enable custom REST service setting [638](#)
- enable file checkout [602](#)
- enable icons on locked objects [623](#)
- environment migration [612](#), [865](#)
- filtered list view
 - concurrent exports [632](#)
 - displaying initial results [628](#)
 - editable fields [632](#)
 - enable object type and field export choices [629](#)
 - export to Excel [629](#)
 - fields for advanced filters [629](#)
 - number of levels to export [632](#)
 - object types to exclude from bulk update [631](#)
 - object types to exclude in export [629](#), [630](#)
 - profiles to prevent from bulk updating [631](#)
 - profiles to prevent from exporting [630](#)
- format of object names [610](#)
- global unlock [623](#)
- hide menu items [608](#)
- home page [625](#)
- home page filtered lists [625](#), [627](#), [628](#)
- home page number of embedded reports [626](#)
- home page number of objects in a table [627](#)
- home page number of reports [627](#)
- home page order of predefined tables [625](#)
- host setting [640](#)
- illegal characters [635](#)
- internal page size for search results [666](#)

settings (*continued*)

- language analyzer used by search [663](#)
- legacy move behavior [640](#)
- localization [639](#)
- localization settings [639](#)
- lock [619](#)
- lock and unlock objects [621](#)
- lock menu [622](#)
- lock menu for display [621](#)
- locking a user account [644](#)
- mail server address [612](#)
- Maximum Import Rows [635](#)
- Maximum Import Rows setting [635](#)
- modify menu order [607](#)
- network connection request timeout [668](#)
- New User Default Locale [605](#)
- number of allowed connections [669](#)
- number of allowed connections per host [668](#)
- number of attempts to fill the search results [665](#)
- number of records inserted per batch [664](#)
- number of records to cache [661](#), [662](#)
- number of request attempts [669](#)
- number of search results records cached per user session [666](#)
- object reset ACL restrictions [624](#)
- object reset locking restrictions [625](#)
- object reset logging level [624](#)
- object reset on error behavior [624](#)
- object resets [624](#)
- objects in listing pane [614](#)
- optimizing file uploads [613](#)
- page size [605](#)
- path to global search administration server [660](#)
- path to server for search indexing [660](#)
- phonebook bucket size [605](#)
- Platform folder [638](#)
- Platform Reporting Framework folder [642](#)
- Platform Reporting Schema folder [642](#)
- Platform Security folder [644](#)
- polling interval [662](#)
- progress refresh interval [661](#)
- query path to the Apache Solr server [663](#)
- query path to the Apache Solr server for Folder ACL indexing [663](#)
- query path to the Apache Solr server that handles Folder ACL search requests [665](#)
- report fragments [612](#)
- reporting framework
 - adding namespaces [963](#)
 - custom forms [960](#)
- reporting framework namespaces [963](#)
- reporting schema
 - add indexes [642](#)
- Reports Access Page Size [605](#)
- security log off link [644](#)
- security safe tags [646](#)
- selectors to use for search [607](#)
- show field guidance [600](#)
- show hidden [602](#)
- show system generated field guidance [600](#)
- signature [619](#)
- signature locks [620](#)
- signatures [619](#)
- socket timeout for indexing [669](#)

settings (*continued*)

- socket timeout for searching [670](#)
- sort list views by modification date [602](#)
- SOXDocument auto-naming objects [611](#)
- submenus [607](#)
- system security model [635](#)
- task focused UI
 - disable bulk update [630](#)
- time to search before timing out [667](#)
- triangle object relationships [955](#), [959](#)
- URL of the Apache Solr server for Folder ACL indexing [664](#)
- URL of the Apache Solr server for search requests [666](#)
- URL path to the Apache Solr server for search requests [665](#)
- use legacy associate [635](#)
- User Preferences folder [648](#)
- user provisioning [603](#)
- Users Can Copy Access From [605](#)
- White-listed Suspicious Character Combinations [647](#)
- Settings
 - modifying in the Standard UI [598](#)
 - modifying in the Task Focused UI [597](#)
- signature and lock settings [619](#)
- signature links for sign off [619](#)
- signature settings [619](#)
- simple string
 - data type [203](#)
- single file
 - data type [203](#)
- solution schema visualization editor
 - about [250](#)
 - using [250](#)
- solution schema visualizations
 - creating [252](#)
- sosa properties and parameters [1084](#)
- SOXBusEntity objects
 - best practices for limiting [1111](#)
- specifying a primary parent ID [983](#)
- specifying connector currency values [986](#)
- specifying connector date values [986](#)
- SSL, *See* TLS
- SSL certificate
 - Ascent [1039](#)
 - Reg-Track [1049](#)
 - regulatory feeds [61](#)
 - SecurityScorecard [1035](#), [1071](#)
 - Supply Wisdom [1073](#)
 - Thomson Reuters [1043](#)
- ssoRequiresSSL [786](#)
- Standard UI
 - compared to Task Focused UI [365](#)
 - permissions [363](#)
 - URL and URL redirects [363](#)
- starting and stopping
 - Framework Model Generator service [850](#)
 - IBM Cognos service [849](#), [850](#)
- starting groups
 - best practices [1113](#)
- static IP address [777](#)
- storage backup
 - enable and disable [685](#), [722](#)
- storage location
 - OPBackup [718](#)

- String Concatenation Utility
 - about [752](#)
 - running [752](#)
 - SQL file [754](#)
- string data types [137](#)
- sub-groups
 - removing [89](#)
- Super Administrator [75](#)
- Supply Wisdom [1073](#)
- System Admin Mode
 - enabling and disabling [71](#)
- system fields
 - localizing [564](#)
- system file management
 - checking in files [197](#)
 - checking out files [197](#)
 - copying files [194](#)
 - creating folders [193](#)
 - deleting files [195](#)
 - download files [196](#)
 - moving files [194](#)
 - overview [187](#)
 - refreshing trigger configurations [198](#)
 - renaming files [194](#)
 - tasks [191](#)
 - uploading files [193](#)
 - uploading modified files [197](#)
- System files
 - adding and modifying in the Task Focused UI [195](#)
- System files and folders
 - managing in the Task Focused UI [191](#)
- system generated field guidance [600](#)
- system notice
 - login screen [571](#)

T

- tab
 - Dashboard tab [319–321](#)
 - My Work tab [313](#)
- tabbed interface, Home page [309](#)
- tabs
 - add reports [311](#)
 - hide [312](#)
 - unhide [312](#)
- Task Focused UI
 - adding business entity selector fields to views [412](#)
 - adding Natural Language Classifier (object association suggestions) [430](#)
 - adding Natural Language Classifier (taxonomy suggestions) [410](#)
 - compared to Standard UI [365](#)
 - configuring [363](#)
 - configuring GRC Workflow [495](#)
 - Dashboards [367](#)
 - defining a Creation View [391](#)
 - defining a dashboard for a profile [367](#)
 - defining a Grid View [389](#)
 - defining a Task View [394](#)
 - defining a theme [454](#)
 - defining default filters for Grid Views [406](#)
 - defining editable and readonly rules [440](#)
 - defining Greater, GreaterEqual, Less, LessEqual, and Equal rules [443](#)

- Task Focused UI (*continued*)
 - defining MinLength and MaxLength rules [444](#)
 - defining pattern rules [445](#)
 - defining required rules in views [442](#)
 - defining rules in views [439](#)
 - defining warnings in views [445](#)
 - designing a Creation View [377](#)
 - designing a Grid View [374](#)
 - designing a Task View [382](#)
 - exporting and importing dashboards [452](#)
 - fields in views [372](#)
 - general elements in the View Designer [399](#)
 - inline guidance [400](#)
 - JSON tips for editing [398](#)
 - permissions [363](#)
 - planning Creation Views [376](#)
 - planning Grid Views [373](#)
 - planning Task Views [380](#)
 - supported field value colors [409](#)
 - system views [370](#)
 - Task View header [404](#)
 - themes [452](#)
 - URL and URL redirects [363](#)
 - user guidance [402](#)
 - using a Creation View [377](#)
 - using a Grid View [373](#)
 - using a Task View [381](#)
 - using the View Designer [385](#)
 - views [370](#)
- Task View header
 - adding to views in the Task Focused UI [404](#)
- Task Views
 - adding a card layout [414](#)
 - adding a chart diagram [416](#)
 - adding a classifier field that makes object association suggestions [430](#)
 - adding a classifier field that makes taxonomy suggestions [410](#)
 - adding a count [424](#)
 - adding a grid layout [425](#)
 - adding a header [404](#)
 - adding a tree diagram [429](#)
 - adding actions to relationship fields [434](#)
 - applying colors to enumerated fields [407](#)
 - applying colors to value ranges [408](#)
 - arranging fields in columns [400](#)
 - defining a Delete action [438](#)
 - defining a Get Watson Classifier action [438](#)
 - defining a Recursive Copy action [436](#)
 - defining an Add New action [435](#)
 - defining an Associate action [434](#)
 - defining an Associate Primary Parent action [435](#)
 - defining dynamic filters on relationship fields [438](#)
 - defining in the Task Focused UI [394](#)
 - designing in the Task Focused UI [382](#)
 - designing to use with GRC Workflow [505](#)
 - displaying a number field as a progress bar [410](#)
 - displaying a URL field as a button or link [410](#)
 - planning in the Task Focused UI [380](#)
 - using in the Task Focused UI [381](#)
- task-oriented hyperlinking [1113](#)
- techniques for Security Directory Integrator [988](#)
- template models, using in the reporting framework [961](#)
- test deployment [865](#)

- test environment
 - refreshing from production data [694](#), [696](#), [736](#)
- text
 - application [564](#)
 - object [561](#)
- Theme Deployer [1065](#)
- themes [1067](#)
- Themes
 - defining in the Task Focused UI [454](#)
 - system and custom [452](#)
- Third Party Risk Management
 - SecurityScorecard [1071](#)
 - Supply Wisdom [1073](#)
- threadpool sizing
 - application server [821](#)
- time-out period, browser [836](#)
- timesheets [993](#)
- TLS
 - accessing the OpenPages application [783](#)
 - Apache load balancer server configuration [794](#), [795](#)
 - Apache Web Server configuration [789–791](#)
 - certificate renewal [804](#)
 - Cognos [798](#)
 - Cognos certificate renewal on Apache Web Server [805](#)
 - Cognos certificate renewal on IIS [804](#)
 - configuration [783](#)
 - IBM HTTP server [796](#)
 - IBM HTTP server configuration [791–793](#), [796–798](#)
 - LDAP configuration [81](#)
 - Linux load balancer server configuration [791](#)
 - Microsoft IIS configuration [787–790](#)
 - properties files configuration [798](#)
 - WebSphere certificate renewal [806](#)
 - WebSphere configuration [61](#), [783](#), [785](#), [786](#), [1031](#), [1035](#), [1039](#), [1043](#), [1049](#), [1055](#), [1071](#), [1073](#)
- Tomcat heap size
 - reporting server [821](#)
- tools properties [1085](#)
- track configuration changes [770](#)
- triangle relationships [109](#)
- troubleshooting
 - contacting IBM Support [1099](#)
 - exchanging information with IBM Support [1100](#), [1101](#)
 - Export JSON [1106](#)
 - fixes
 - installing [1099](#)
 - getting fixes [1099](#)
 - identifying problems and techniques [1097](#)
 - known problems for browsers [836](#)
 - known problems for the QRadar integration package [1105](#)
 - required fields [1106](#)
 - SDI error messages [1105](#)
 - searching knowledge bases [1098](#)
 - security domains included in search [1106](#)
 - subscribing to Support notifications [1101](#)
- troubleshooting the Connection Refused error message [989](#)
- tuning
 - Db2 database [822](#)
 - reporting service [821](#)

U

- UAT deployment [865](#)

- UCF [986](#)
- unlock all icon [623](#)
- unlocking business entities [623](#)
- update data using FastMap [915](#)
- UPEA tool
 - syntax [102](#)
- uploading large files [613](#), [617](#)
- URL for application
 - shortening [815](#)
 - Standard UI [363](#)
 - Task Focused UI [363](#)
- user accounts
 - configuring LDAP access for [81](#), [82](#)
 - copying access [87](#)
 - creating [84](#)
 - modifying [86](#)
- user administration [73](#)
- user guidance
 - adding to views in the Task Focused UI [402](#)
- user name format [568](#)
- user names
 - exclude characters from [635](#)
 - rules [84](#)
- user names in a phonebook [358](#)
- User Preferences folder settings [648](#)
- user provisioning
 - Copy Access From Inactive [603](#)
 - Copy User Info Attributes [604](#)
 - Copy User Info Choice [604](#)
 - Default Allowed Profiles [604](#)
 - Default User Change Password [604](#)
 - Default User Password Expiration [605](#)
 - New User Default Locale [605](#)
 - Reports Access Page Size [605](#)
 - Users Can Copy Access From [605](#)
- user provisioning settings [603](#)
- User Roles
 - Using groups to establish [1090](#)
- User Selector [358](#)
- user-defined keys [576](#)
- User/Group Selector [358](#)
- users
 - associating profiles [302](#)
 - disassociating profiles [304](#)
- Users Can Copy Access From setting [605](#)
- users table
 - updating to change passwords [102](#)
- using complex logic in a search filter [274](#)
- using OPBackup and Op Restore with global search [653](#)
- using the QRadar integration project [982](#)
- utilities
 - about back up and restore [690](#)
 - about backup and restore [679](#), [713](#)
 - CommandCenter Backup [687](#)
 - CommandCenter Restore [727](#)
 - Entity Move/Rename [708](#), [758](#)
 - Entity Move/Rename input file [710](#), [759](#)
 - filtering on long string indexes [702](#), [746](#)
 - OPBackup [682](#), [718](#)
 - OpenPages CommandCenter Backup [724](#)
 - OpenPages CommandCenter Restore [689](#)
 - OPRestore [686](#), [723](#)
 - running OPBackup [719](#)
 - running OPBackup live [684](#), [721](#)

utilities (*continued*)

- running OPCCBackup [687, 695, 726](#)
- running OPCCRestore [689, 728](#)
- running OPRestore [686, 723](#)
- running string concatenation [752](#)
- String Concatenation [752](#)
- string concatenation SQL file [754](#)

V

validating

- rules [142](#)

validation rules in the Task Focused UI

- defining warnings [445](#)

verify

- encryption algorithm [100](#)

View Designer

- adding a card layout [414](#)
- adding a chart diagram [416](#)
- adding a count [424](#)
- adding a grid layout [425](#)
- adding a tree diagram [429](#)
- adding actions to relationship fields [434](#)
- defining a Delete action [438](#)
- defining a Get Watson Classifier action [438](#)
- defining a Recursive Copy action [436](#)
- defining an Add New action [435](#)
- defining an Associate action [434](#)
- defining an Associate Primary Parent action [435](#)
- defining default filters for Grid Views [406](#)
- defining dynamic filters on relationship fields [438](#)
- displaying a number field as a progress bar [410](#)
- displaying a URL field as a button or link [410](#)
- supported field value colors [409](#)
- user guidance [402](#)
- using in the Task Focused UI [385](#)

View Designer)

- adding a classifier field that makes object association suggestions [430](#)
- adding a classifier field that makes taxonomy suggestions [410](#)
- general elements [399](#)

views

- copy to profile [330](#)
- setting default [329](#)

W

Watson certificate [1031](#)

web server

- certificate authority approval [788, 790](#)

webAppSecurity [786](#)

WebSphere

- configuring certificates [61, 1031, 1035, 1039, 1043, 1049, 1055, 1071, 1073](#)
- generating the CSR file [783](#)
- importing certificate into Java [785](#)
- importing certificates [783](#)
- TLS configuration [786](#)
- TLS ports on virtual hosts [783](#)

what's new [1](#)

White-listed Suspicious Character Combinations [647](#)

Windows services

Windows services (*continued*)

- starting [841](#)

- stopping [843](#)

Wolters Kluwer certificate [1055](#)

workbook. See FastMap. [916](#)

X

XSS

- cross-site scripting filter setting [645](#)

- Safe Tags setting [646](#)

